AFF and FAS Switch Documentation

Cluster and storage switches

NetApp
October 03, 2022

Table of Contents

AFF and FAS Switch Documentation

Broadcom-supported BES-53248 switches

Overview of Broadcom-supported BES-53248 cluster switches

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 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.

BES-53248 cluster switch port assignments

You can use the Broadcom-supported BES-53248 cluster switch port assignments table as a guide to configuring your cluster.

Switch ports	Ports usage
01-16	10/25GbE cluster port nodes, base configuration
17-48	10/25GbE cluster port nodes, with licenses
49-54	100GbE cluster port nodes, with licenses, added right to left
55-56	100GbE cluster Inter-Switch Link (ISL) ports, base configuration

Port group speed constraint

On BES-53248 cluster switches, the 48 10/25GbE (SFP28/SFP+) ports are combined into 12 x 4-port groups as follows:

- Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44, and 45-48.

The SFP28/SFP+ port speed must be the same (10GbE or 25GbE) across all ports in the 4-port group.

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.

Document title	Description
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
NetApp 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.

Configure your BES-53248 cluster switches

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

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
   - 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.

```
(cs2)# show serviceport
Interface Status............................... Up
IP Address..................................... 172.19.2.2
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 172.19.2.254
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................
fe80::dac4:97ff:fe71:123c/64
IPv6 Default Router............................ fe80::20b:45ff:fea9:5dc0
Configured IPv4 Protocol....................... DHCP
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... D8:C4:97:71:12:3C
```

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!
```

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

> 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
--------------------------------------------------------------------
 unit      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.

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.4.4.6.stk active
Remote Password:**

Mode........................................... SFTP
Set Server IP.................................. 172.19.2.1
Path........................................... //tmp/
Filename....................................... EFOS-3.4.4.6.stk
Data Type...................................... Code
Destination Filename........................... active

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


File transfer operation completed successfully.
```

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
Serial Number.................................. QTFCU38260023
Maintenance Level.............................. A
Manufacturer................................... 0xbc00
Burned In MAC Address.......................... D8:C4:97:71:0F:40
Software Version............................... 3.4.4.6
Operating System............................... Linux 4.4.211-28a6fe76
Network Processing Device...................... BCM56873_A0
CPLD Version................................... 0xff040c03

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:

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

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

6. Verify that the new switch software is installed: `show bootvar`

```
(cs2)# show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active      backup   current-active  next-active
----    ----------- -------- --------------- ------------
1     3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(cs2) #
```

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

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`

```
(cs2)# show license
Reboot needed.................................. No
Number of active licenses...................... 0

License Index  License Type     Status
-------------- ---------------- -----------

No license file found.
```

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.

```
(cs2)# copy sftp://root@172.19.2.1/var/lib/tftpboot/license.dat
nvram:license-key 1
Remote Password:**

Mode........................................... SFTP
Set Server IP.................................. 172.19.2.1
Path........................................... /var/lib/tftpboot/
Filename....................................... license.dat
Data Type...................................... license

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...


License Key transfer operation completed successfully. System reboot is
required.
```

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

   `show license`

```
(cs2)# show license

Reboot needed.................................. Yes
Number of active licenses...................... 0


License Index  License Type      Status
-------------- ----------------- -------------------------------
1              Port              License valid but not applied
```

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)# 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
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
0/55             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
```

```
(cs2)# show license

Reboot needed.................................. No
Number of installed licenses................... 1
Total Downlink Ports enabled................... 16
Total Uplink Ports enabled..................... 8

License Index  License Type               Status
-------------- -------------------------
-----------------------------------
1              Port                       License applied
```

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
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
```

When installing additional licenses, you must configure the new interfaces manually. Re-applying an RCF to an existing working production switch is not advisable.

Restrictions and limitations

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` and `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
LICENSING :
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.

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
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 sftp://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.......................................... SFTP
Set Server IP................................. 172.19.2.1
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

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

File transfer operation completed successfully.
```

Depending on your environment, you might need to use a double slash in the `copy` command, for example: `copy sftp://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 sftp://172.19.2.1/tmp/BES-53248_RCF_v1.6-Cluster-HA.txt nvram:script RCF_v1.6-Cluster-HA.scr`.

The file name must not include the symbols `\/:*?"<>|` and the maximum length allowed is 32 chars.

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

   `script list`

```
(cs2)# script list

Configuration Script Name                    Size(Bytes)  Date of
Modification
-----------------------------------------  -----------
--------------------
BES-53248_RCF_v1.6-Cluster-HA.scr        2241        2020 09 30
05:41:00

1 configuration script(s) found.
```

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      Type   Mode      Mode         Status     Status Trap    Mode
Timeout
--------- ------ --------- ---------- ---------- ------ ------- ------
--------
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                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
0/49               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
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!
```

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.

Before you begin

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.

Enable SSH on BES-53248 cluster 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)# 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!
```

2. Verify that SSH is enabled:

   `show ip ssh`

```
(switch)# show ip ssh

SSH Configuration

Administrative Mode: .......................... Enabled
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
```

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. 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` 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::*>
```

2. 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` 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.
```

The log collect command is not available at this time. See Bug 1225042 for further details.

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

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 *NetApp 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 Install the Cluster Switch Health Monitor (CSHM) configuration file and Configure the cluster switch log collection feature 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

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`

```
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_clus2   true
```

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:

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  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 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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

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
e0b     true
```

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
Local Interface................................ 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 *NetApp 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
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     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

Local Interface................................ 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
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
```

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

`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         e0b
true
```

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 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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

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     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     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 *NetApp 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 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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

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:

```
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
```

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     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. 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:

```
cluster1::*> network device-discovery show -protocol cdp
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 Install the Cluster Switch Health Monitor (CSHM) configuration file and Configure 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

Hardware Universe

Broadcom-supported BES-53248 switches setup and configuration

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 Broadcom-supported BES-53248 switches setup and configuration 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 Install the Cluster Switch Health Monitor (CSHM) configuration file and Configure the cluster switch log collection feature 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 *NetApp Hardware Universe* contains information about ONTAP compatibility, supported EFOS firmware, and cabling to BES-53248 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 *NetApp 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.

   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. 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
Local Interface................................ 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
Local Interface................................ 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
```

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            0/55     176       R            BES-53248   0/55
cs2            0/56     176       R            BES-53248   0/56
```

The following example lists the neighboring devices on switch cs2:

```
(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
-------------- -------- --------- ------------ ----------- ---------
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
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

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
```

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 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
```

8. 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_clus2   true
```

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.

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 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
```

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:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
```

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 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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

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 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
```

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
Device ID      Intf         Holdtime  Capability   Platform -- Port ID
-------------- ------------ --------- ------------ -----------
----------
node1          0/1          175       H            FAS2750     e0a
node2          0/2          157       H            FAS2750     e0a
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       H            FAS2750     e0b
node2          0/2          179       H            FAS2750     e0b
cs1            0/55         175       R            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`

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
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:

    `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:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                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 Install the Cluster Switch Health Monitor (CSHM) configuration file and Configure 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 Hardware Universe

Broadcom-supported BES-53248 switches setup and configuration

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.

Before you begin

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 *NetApp Hardware Universe* for the actual cluster ports supported on your platform.
- 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:

```
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    Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b    Cluster      Cluster          up   9000  auto/10000 healthy
false
```

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:

```
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      169.254.217.125/16  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
```

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

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

--------------------------------------------------------------------
 unit      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.

```
(cs2)# *copy sftp://root@172.19.2.1//tmp/EFOS-3.4.4.6.stk active*
Remote Password:********

Mode........................................... SFTP
Set Server IP.................................. 172.19.2.1
Path........................................... //tmp/
Filename....................................... EFOS-3.4.4.6.stk
Data Type...................................... Code
Destination Filename........................... active

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


File transfer operation completed successfully.
```

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
Serial Number.................................. QTFCU38260023
Maintenance Level.............................. A
Manufacturer................................... 0xbc00
Burned In MAC Address.......................... D8:C4:97:71:0F:40
Software Version............................... 3.4.4.6
Operating System............................... Linux 4.4.211-28a6fe76
Network Processing Device...................... BCM56873_A0
CPLD Version................................... 0xff040c03

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:

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

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

6. Verify that the new switch software is installed: `show bootvar`

```
(cs2) # show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active      backup   current-active  next-active
----    ----------- -------- --------------- ------------
1     3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(cs2) #
```

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`

```
(cs2)# show license
Reboot needed.................................. No
Number of active licenses...................... 0

License Index  License Type     Status
-------------- ---------------- -----------

No license file found.
```

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.

```
(cs2)# copy sftp://root@172.19.2.1/var/lib/tftpboot/license.dat
nvram:license-key 1
Remote Password:**

Mode........................................... SFTP
Set Server IP.................................. 172.19.2.1
Path........................................... /var/lib/tftpboot/
Filename....................................... license.dat
Data Type...................................... license


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...

License Key transfer operation completed successfully. System reboot is
required.
```

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

   `show license`

```
(cs2)# show license

Reboot needed................................. Yes
Number of active licenses..................... 0


License Index  License Type      Status
-------------- ----------------- -------------------------------
1              Port              License valid but not applied
```

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)# 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
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
0/55             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 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`

```
(cs2)# show license

Reboot needed................................. No
Number of installed licenses.................. 1
Total Downlink Ports enabled.................. 16
Total Uplink Ports enabled.................... 8

License Index  License Type              Status
-------------- -------------------------
----------------------------------
1              Port                      License applied
```

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
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
```

When installing additional licenses, you must configure the new interfaces manually. Re-applying an RCF to an existing working production switch is not advisable.

Restrictions and limitations

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 are: `debug transfer` and `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
LICENSING :
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
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) y
```

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 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 RCF containing only the new port configuration.
  2. Copy the second RCF to the switch.
  3. Apply the script to the switch using the command: `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:

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

9. If desired, configure the SSH server.

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

   a. Generate RSA keys.

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

b. Generate DSA keys (optional)

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

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

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

d. Enable the SSH server.

If necessary, exit the configuration context.

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

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

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

`configure`

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

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

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

12. Configure the switch name:

`hostname cs2`

The switch prompt will display the new name:

```
(Routing)# hostname 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!
```

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 sftp://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........................................... SFTP
Set Server IP.................................. 172.19.2.1
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

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

File transfer operation completed successfully.
```

Depending on your environment, you might need to use a double slash in the copy command, for example: `copy sftp://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 sftp://172.19.2.1/tmp/BES-53248_RCF_v1.6-Cluster-HA.txt nvram:script RCF_v1.6-Cluster-HA.scr`.

The file name must not include the symbols `\/:*?"<>|` and the maximum length allowed is 32 chars.

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

```
script list
```

```
(cs2)# script list

Configuration Script Name                  Size(Bytes)  Date of
Modification
-----------------------------------------  -----------
--------------------
BES-53248_RCF_v1.6-Cluster-HA.scr          2241         2020 09 30
05:41:00

1 configuration script(s) found.
```

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      Type   Mode      Mode         Status     Status Trap    Mode
Timeout
--------- ------ --------- ------------ ---------- ------ ------- ------
-------
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             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
0/49            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
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!
```

Once the RCF is installed on the first switch, repeat these steps to install the RCF on the second cluster switch.

See this KB for further information when installing an RCF for MetroCluster.

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
```

> ℹ️ 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.

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 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. Verify that SSH is enabled:

show ip ssh

```
(switch)# show ip ssh

SSH Configuration

Administrative Mode: .......................... Enabled
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
```

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` 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::*>
```

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` 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.
```

ⓘ The log collect command is not available at this time. See Bug 1225042 for further details.

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

Verify the configuration after a BES-53248 cluster switch upgrade

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:

```
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    Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b    Cluster      Cluster          up   9000  auto/10000 healthy
false
```

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 interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.217.125/16 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
```

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

```
cluster1::> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
```

Replace a Broadcom-supported BES-53248 cluster switch

Replacing a defective Broadcom-supported BES-53248 cluster 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 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 Broadcom-supported 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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false


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


cluster1::> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
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
```

```
(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
------------------------ --------- --------- ---------- ----------------
---------
node1                    0/1       175       H          FAS2750
e0a
node2                    0/2       152       H          FAS2750
e0a
cs2                      0/55      179       R          BES-53248
0/55
cs2                      0/56      179       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       129       H          FAS2750
e0b
node2                    0/2       165       H          FAS2750
e0b
cs1                      0/55      179       R          BES-53248
0/55
cs1                      0/56      179       R          BES-53248
0/56
```

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
(newcs2)#
```

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
Vserver   Interface    Auto-revert
--------- ------------ ------------
Cluster   node1_clus1  true
Cluster   node1_clus2  true
Cluster   node2_clus1  true
Cluster   node2_clus2  true
```

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)(interface 0/55-0/56)# exit
(cs1)# show port-channel 1/1

Local Interface................................ 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
```

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 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       Cluster      Cluster          up   9000  auto/10000  healthy
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
e0b       Cluster      Cluster          up   9000  auto/auto   -
false
```

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

   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 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      e0a
false
```

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   Epsilon
------ -------- ------------  --------
node1  true     true          true
node2  true     true          true
```

11. Confirm the following cluster network configuration:

    `network port show`

```
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       Cluster     Cluster          up   9000  auto/10000  healthy
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
e0b       Cluster      Cluster          up   9000 auto/10000  healthy
false


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.
```

```
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    H           FAS2980       e0a
node2                Eth1/2         145    H           FAS2980       e0a
newcs2(FDO296348FU)  Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
newcs2(FDO296348FU)  Eth1/66        176    R S I s     N9K-C92300YC
Eth1/66


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    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66
```

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    Holdtime    Capability    Platform    Port ID
---------    ----    --------    ----------    --------    --------
node1        0/1     175         H             FAS2750     e0a
node2        0/2     152         H             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         H             FAS2750     e0b
node2        0/2     165         H             FAS2750     e0b
cs1          0/55    179         R             BES-53248   0/55
cs1          0/56    179         R             BES-53248   0/56
```

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

Broadcom-supported BES-53248 switches setup and configuration

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.

Replace a Cisco Nexus 3132Q-V Cluster Switch	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 pass-through 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

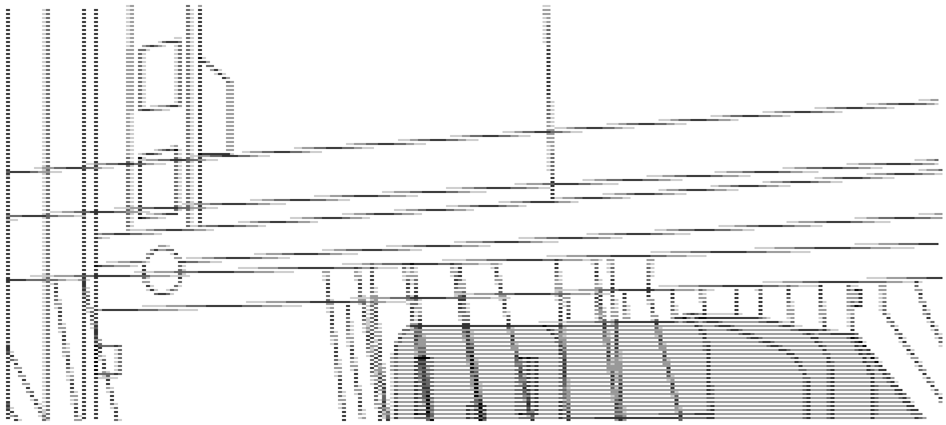
     a. Determine the vertical location of the switches and blanking panel in the cabinet.

        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.

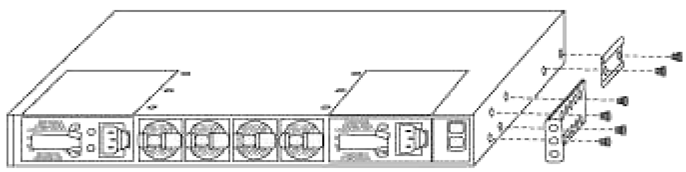
     d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



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.

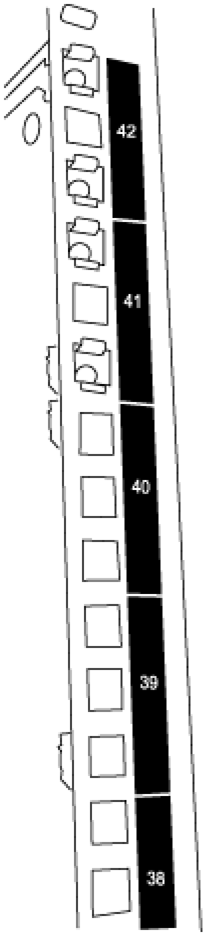
   

   b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.

   c. Install the rear rack-mount bracket on the switch chassis.

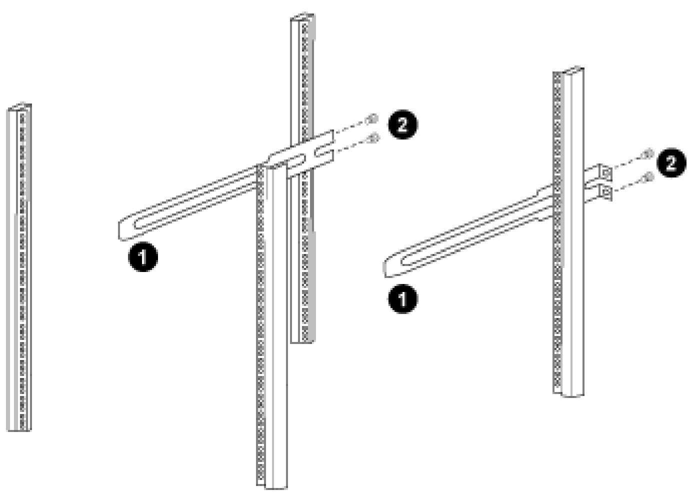
   d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.

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.



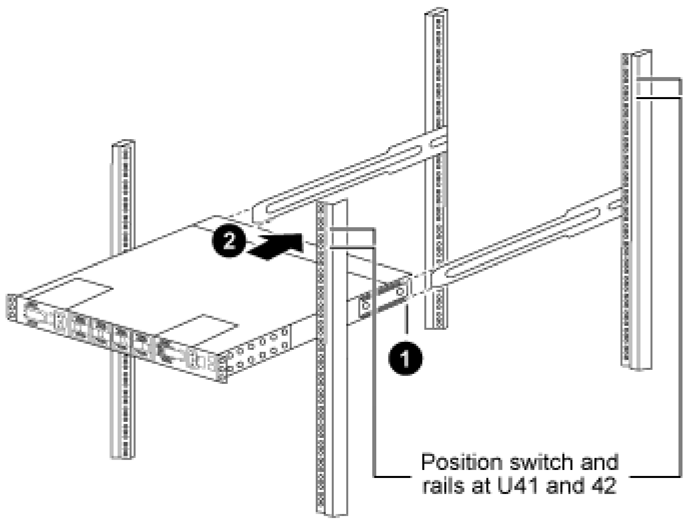
      1. As you gently slide the slider rail, align it to the screw holes in the rack.
      2. Tighten the screws of the slider rails to the cabinet posts.
   b. Repeat step 4a for the right side rear post.

c. Repeat steps 4a and 4b at the RU41 locations on the cabinet.

5. Install the switch in the cabinet.

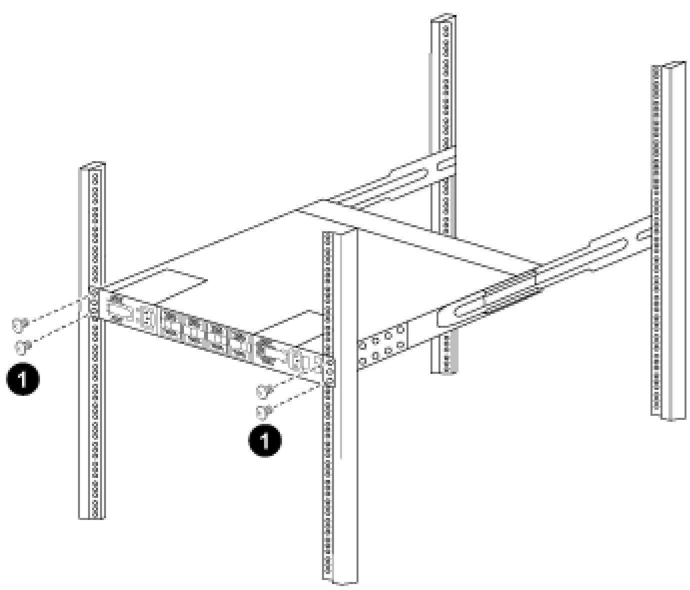
> ⓘ This step requires two people: one person to support the switch from the front and another to guide the switch into the rear slider rails.

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 *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.
Cisco Nexus 3232C in a NetApp system cabinet	See the *Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet* guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the *Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet* 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 set-privilege 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 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 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.

Initial setup

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

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

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

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  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. Check the administrative or operational status of each cluster interface.
   a. Display the network port attributes:

      `network port show –ipspace Cluster`

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02
                                                 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: 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
```

   b. Display information about the LIFs:

      `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
            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
```

5. Ping the remote cluster LIFs:

```
cluster ping-cluster -node local
```

```
cluster1::*> cluster ping-cluster -node local
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
```

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 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 SFTP being used to 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
14:00:37]

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(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-
Version          Upg-Required
------------ ----------- ---------------------------------------
-------------------- ------------
     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.
[] 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 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.
> - Before you perform this procedure, make sure that you have a current backup of the switch configuration.

Steps

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

   `network device-discovery show`

```
cluster1::*> network device-discovery show
Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- -----------------
------------
cluster1-01/cdp
             e0a    cs1                       Ethernet1/7       N3K-
C3132Q-V
             e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster1-02/cdp
             e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
             e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster1-03/cdp
             e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
             e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
             e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
             e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V
cluster1::*>
```

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 -ipspace Cluster`

```
cluster1::*> network port show -ipspace 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/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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
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 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: cluster1-04
```

```
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
cluster1::*>
```

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

`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
            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  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
            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
cluster1::*>
```

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    10.0.0.1
NX3132QV
     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    10.0.0.2
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.
```

For ONTAP 9.8 and later, use the command `system ethernet switch show -is -monitoring-enabled-operational true`.

3. Disable auto-revert on the cluster LIFs.

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

Ensure that auto-revert is disabled after running this command.

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 -vserver Cluster`

```
cluster1::*> 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      169.254.3.4/23     cluster1-01
e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23     cluster1-01
e0a     false
            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
e0a     false
            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
e0a     false
            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     false
cluster1::*>
```

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
cluster1::*>
```

7. If you do not already have a current backup of the switch, you can save the current switch configuration by

copying the output of the following command to a log file:

```
show running-config
```

8. 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.
9. 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)...
```

10. 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-config
echo-commands
```

11. 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-
4,
* 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
*
*****************************************************************************
******
```

12. 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.

13. 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.

```
cs2# copy running-config startup-config
[########################################] 100% Copy complete
```

14. 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
```

15. 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
```

16. Verify the health of cluster ports on the cluster.

    a. Verify that cluster ports are up and healthy across all nodes in the cluster:

    `network port show -ipspace Cluster`

```
cluster1::*> network port show -ipspace 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      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: cluster1-03

Ignore
                                                 Speed(Mbps) Health
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
healthy false

Node: cluster1-04

Ignore
                                                 Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

b. Verify the switch health from the cluster.

```
cluster1::*> network device-discovery show -protocol cdp
Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/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
cluster01-3/cdp
             e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
             e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
             e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
             e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ---------------- -----
cs1                         cluster-network    10.233.205.90    N3K-
C3132Q-V
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    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.
```

For ONTAP 9.8 and later, use the command `system ethernet switch show -is -monitoring-enabled-operational true`.

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.
```

17. 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
```

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

    `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
            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
            cluster1-02_clus1  up/up      169.254.3.8/23     cluster1-02
e0d     false
            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
e0b     false
            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
e0b     true
cluster1::*>
```

19. 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 displayed.
cluster1::*>
```

20. Repeat Steps 7 to 16 on switch cs1.
21. Enable auto-revert on the cluster LIFs.

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

22. 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
```

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

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      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)
--
.
.
```

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

```
show port-channel summary
```

```
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      Eth1/31(P)   Eth1/32(P)
cs1#
```

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

`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
            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
e0b     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
e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23     cluster1-04
e0b     true
cluster1::*>
```

26. 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
cluster1::*>
```

27. 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)
```

28. 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` 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.

29. 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` 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.

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

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. 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
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 interface show -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
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

3. 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

   `NX3132_RCF_v1.1_24p10g_26p40g.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
```

```
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    R S I s     N3K-C3132Q-V
Eth1/31
C2                 Eth1/32        174    R S I s     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    R S I s     N3K-C3132Q-V
Eth1/31
C1                 Eth1/32        178    R S I s     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`

```
cluster::*> network interface show -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            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 were displayed.
```

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_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)
```

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      Cluster          up   9000 auto/40000  -        -
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.

```
cluster::*> network interface show -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
            n1_clus2   up/up      10.10.0.2/24       n1            e4e
true
            n2_clus1   up/up      10.10.0.3/24       n2            e4a
true
            n2_clus2   up/up      10.10.0.4/24       n2            e4e
true
4 entries were displayed.
```

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-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 interface show -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
            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 were displayed.
```

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.

```
cluster::*> network interface show -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
            n1_clus2   up/up      10.10.0.2/24       n1            e4e
true
            n2_clus1   up/up      10.10.0.3/24       n2            e4a
true
            n2_clus2   up/up      10.10.0.4/24       n2            e4e
true
4 entries were displayed.
```

31. Verify that all of the cluster interconnect ports are in the `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      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`

```
    cluster::*> network device-discovery show
            Local  Discovered
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

Switch                      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.

```
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

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`

```
cluster::> network device-discovery show
             Local  Discovered
Node         Port   Device              Interface         Platform
----------- ------ ------------------- -----------------
----------------
n1          /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
n4          /cdp
             e4a    CL1                 Ethernet1/8      N3K-C3132Q-V
             e4e    CL2                 Ethernet1/8      N3K-C3132Q-V

12 entries were displayed
```

3. 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
```

```
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
Port      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 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

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: n4
```

```
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  -
-
12 entries were displayed.
```

b. Display information about the logical interfaces:

```
network interface show
```

```
cluster::*> network interface show -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
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
e0a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e0e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e0a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e0e     true

12 entries were displayed.
```

c. Display the information on the discovered cluster switches:

```
system cluster-switch show
```

```
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

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`

```
cluster::*> network interface show -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               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
            n3_clus1   up/up      10.10.0.9/24       n3               e4a
true
            n3_clus2   up/up      10.10.0.10/24      n3               e4a
false
            n4_clus1   up/up      10.10.0.11/24      n4               e4a
true
            n4_clus2   up/up      10.10.0.12/24      n4               e4a
false
12 entries were displayed.
```

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
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
Cluster n3_clus1 n4     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)
```

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.

```
CL1# 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)
```

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 port-channel.

```
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)
```

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.

```
cluster::*> network interface show -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            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
12 entries were displayed.
```

18. Verify that the cluster ports are connected:

`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
--------- ------------ ---------------- ---- ---- ----------- --------
------
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
Port      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 -        -
e0d       Cluster      Cluster          up   9000  auto/10000 -        -

Node: n3

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: n4

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  -        -
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
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
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`

```
cluster::> network device-discovery show
            Local  Discovered
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 displayed.
```

```
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  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
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 -
-
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      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
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
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

```
cluster::*> network interface show -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
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
12 entries were displayed.
```

```
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)I4(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

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

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 break-out 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::> network device-discovery show
            Local  Discovered
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 were displayed.
```

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:

```
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  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
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 -
-
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.
```

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:

```
cluster::*> network interface show -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
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.
```

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
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

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:

```
cluster::*> network interface show -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            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
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 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_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
```

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:

```
Example
CL1# 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      Eth1/41(D)   Eth1/42(D)   Eth1/43(D)
                                    Eth1/44(D)   Eth1/45(P)   Eth1/46(P)
                                    Eth1/47(P)   Eth1/48(P)
```

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)
       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)
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.

```
cluster::*> network interface show -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            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.
```

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  -        -
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      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 -        -
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_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 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:

```
 (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            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 entries were displayed.

----- ------- ----
```

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)# exit
C2#
```

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.

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
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.
```

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:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

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     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

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  -        -
e0c       Cluster      Cluster          up   9000 auto/10000  -        -
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 -        -
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.
```

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_clus4
```

35. Verify that the interface is home:

```
network interface show
```

The following example shows the status of cluster interconnect interfaces is `up` and `Is home` for n1 and n2:

```
cluster::*> network interface show -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            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:

- `network device-discovery show`
- `network port show -role cluster`
- `network interface show -role cluster`
- `system cluster-switch show`

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.

```
cluster::> network device-discovery show
            Local  Discovered
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 displayed.
```

```
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  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
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 -
-
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      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
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
```

```
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

```
cluster::*> network interface show -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
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
12 entries were displayed.
```

```
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

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.
```

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                      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

[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:

```
cluster::> network device-discovery show

       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

8 entries were displayed.
```

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:

```
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.
```

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:

```
cluster::*> network interface show -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       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.
```

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   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

2 entries were displayed.
```

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    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       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

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
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)
```

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
Local Interface................................ 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)
2     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
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.
```

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`:

```
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.
```

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:

```
cluster::*> network interface show -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       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 entries were displayed.
```

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)# exit
C2#
```

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:

```
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 40GbE Node Port
C2(config-if)# spanning-tree port type edge
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.
```

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:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

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     Po1(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
                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.
```

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:

```
cluster::*> network interface show -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       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:

- `network device-discovery show`
- `network port show -role cluster`
- `network interface show -role cluster`
- `system cluster-switch show`

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.

```
cluster::*> network device-discovery show

       Local  Discovered
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 displayed.
```

```
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     -        -

Node: n3
                Broadcast              Speed (Mbps) Health   Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status   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   Status   Health
Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e4a   cluster   cluster    up    9000  auto/40000     -        -
e4e   cluster   cluster    up    9000  auto/40000     -        -

12 entries were displayed.
```

```
cluster::*> network interface show -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       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

12 entries were displayed.
```

```
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

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 pass-through 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

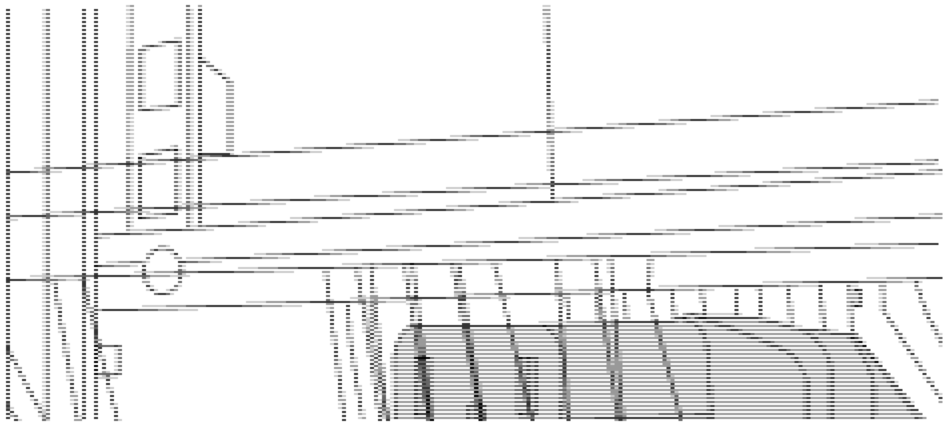
     a. Determine the vertical location of the switches and blanking panel in the cabinet.

        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.

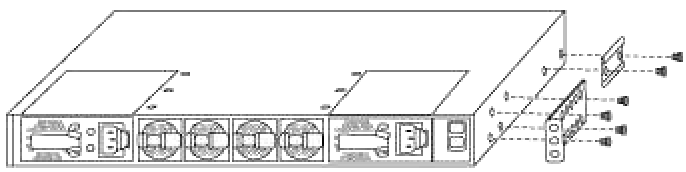
     d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



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.

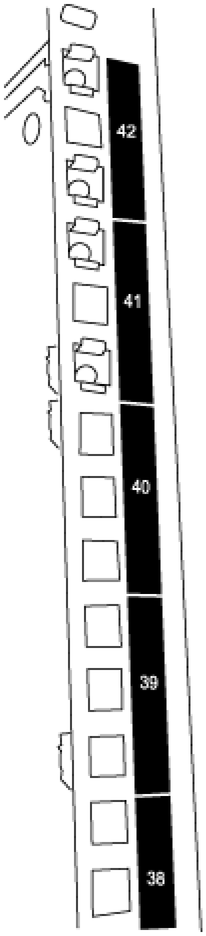
   

   b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.

   c. Install the rear rack-mount bracket on the switch chassis.

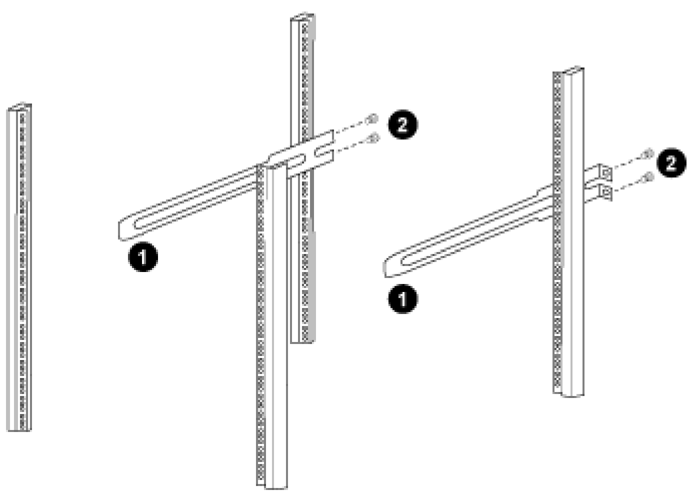
   d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.

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.



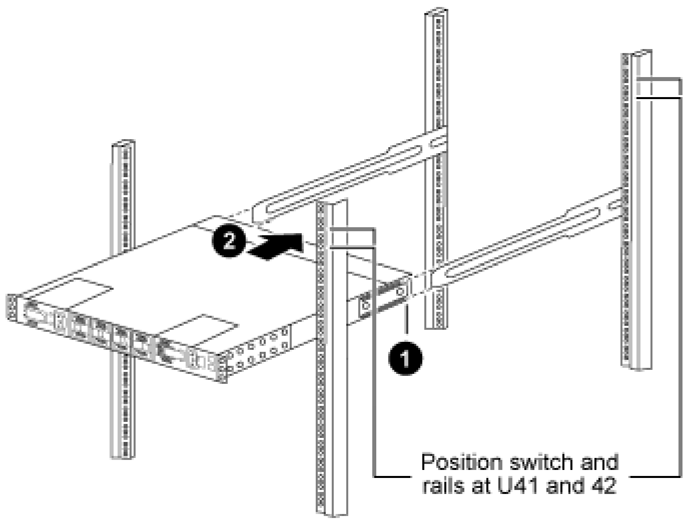
      1. As you gently slide the slider rail, align it to the screw holes in the rack.
      2. Tighten the screws of the slider rails to the cabinet posts.
   b. Repeat step 4a for the right side rear post.

c. Repeat steps 4a and 4b at the RU41 locations on the cabinet.

5. Install the switch in the cabinet.

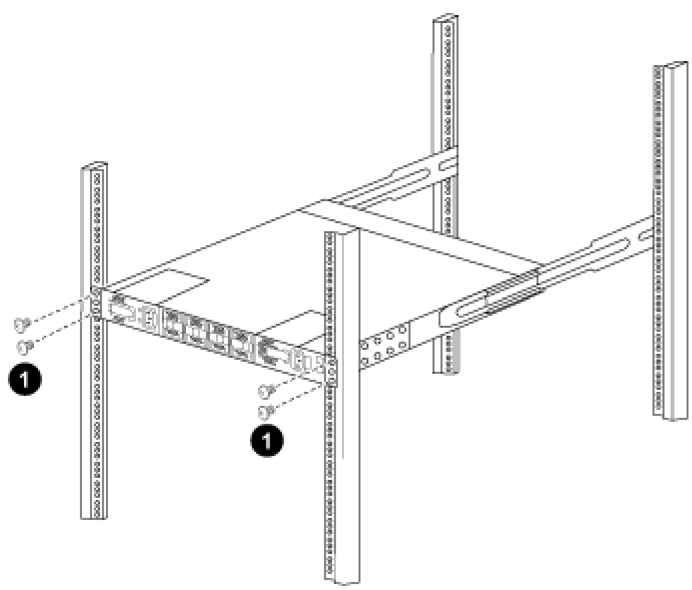
> ⓘ This step requires two people: one person to support the switch from the front and another to guide the switch into the rear slider rails.

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 *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.
Cisco Nexus 3232C in a NetApp system cabinet	See the *Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet* guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the *Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet* 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 set-privilege 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 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 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

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 **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::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------- --------
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`

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02
                                                 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: 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 -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   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 were 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: 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, 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 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
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(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-
Version          Upg-Required
------------ ----------- ---------------------------------------
-------------------- ------------
```

```
     1       nxos        9.3(3)                                    9.3(4)
yes
     1       bios        v08.37(01/28/2020):v08.32(10/18/2016)
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        Type         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            No
     1   SUP   IO FPGA                   0x11        0x12            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.
> - Before you perform this procedure, make sure that you have a current backup of the switch configuration.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches:
   `network device-discovery show`

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------  --------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3232C
            e0d    cs2                       Ethernet1/7       N3K-
C3232C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3232C
            e0d    cs2                       Ethernet1/8       N3K-
C3232C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/1     N3K-
C3232C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/2     N3K-
C3232C
cluster1::*>
```

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/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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
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 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

```
Node: cluster1-04

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
cluster1::*>
```

b. Verify that all the cluster interfaces (LIFs) are on the home port:
`network interface show -role cluster`

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network           Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
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  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
            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 entries were displayed.
cluster1::*>
```

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    10.233.205.92
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`

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------- ------- ----
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     false
            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
e0a     false
            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
e0a     false
            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     false
8 entries were displayed.
cluster1::*>
```

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 displayed.
cluster1::*>
```

7. If you do not already have a current backup of the switch, you can save the current switch configuration by copying the output of the following command to a log file:

   `show running-config`

8. 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.
9. 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)...
```

10. 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
```

11. 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 3232C
* Filename : Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date     : Oct-20-2020
* 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.

```
cs2# copy running-config startup-config
[########################################] 100% Copy complete
```

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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
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      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: cluster1-03

Ignore
                                                  Speed(Mbps) Health
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
healthy false

Node: cluster1-04

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

```
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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::*> network device-discovery show -protocol cdp
Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3232C
            e0d    cs2                       Ethernet1/7       N3K-
C3232C
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3232C
            e0d    cs2                       Ethernet1/8       N3K-
C3232C
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/1     N3K-
C3232C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/2     N3K-
C3232C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ---------------- -----
cs1                         cluster-network    10.233.205.90    N3K-
C3232C
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
```

```
Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    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`

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     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
            cluster1-02_clus1  up/up      169.254.3.8/23     cluster1-02
e0d     false
            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
e0b     false
            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
e0b     true
8 entries were displayed.
cluster1::*>
```

8. 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 displayed.
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
.
.
Eth1/1/1      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`

```
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      Eth1/31(P)   Eth1/32(P)
cs1#
```

14. Verify that the cluster LIFs have reverted to their home port:
`network interface show -role cluster`

```
cluster1::*> **network interface show -role cluster**
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
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
e0b     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
e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23     cluster1-04
e0b     true
8 entries were displayed.
cluster1::*>
```

15. 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 displayed.
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

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

```
cluster::> network device-discovery show

       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

8 entries were displayed.
```

3. Determine the administrative or operational status for each cluster interface.
   a. Display the cluster network port attributes: `network port show -role cluster`

```
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.
```

b. Display information about the logical interfaces: `network interface show -role cluster`

```
cluster::*> network interface show -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       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.
```

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   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

2   entries displayed.
```

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`

```
cluster::*> network interface show -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        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

8 entries were displayed.
```

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
Local Interface................................ 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       Po1(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)
```

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.

```
cluster::*> network interface show -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       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.
```

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`:

```
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.
```

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
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)
```

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:

```
cluster::*> network interface show -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       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 entries were displayed.
```

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)# exit
C2#
```

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:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

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:

```
cluster::*> network interface show -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       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.
```

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
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)
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:

- network device-discovery show
- network port show -role cluster
- network interface show -role cluster
- system cluster-switch show

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.

```
cluster::*> network device-discovery show

       Local  Discovered
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 displayed.
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     -        -

Node: n3
                Broadcast              Speed (Mbps) Health   Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status   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   Status   Health
Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e4a   cluster   cluster    up    9000  auto/40000     -
e4e   cluster   cluster    up    9000  auto/40000     -

12 entries were displayed.

cluster::*> network interface show -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       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

12 entries were displayed.

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)I6(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.
```

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)I6(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 `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 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 break-out 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::> network device-discovery show
            Local  Discovered
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 were displayed.
```

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:

```
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  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
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 -
-
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.
```

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:

```
cluster::*> network interface show -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
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.
```

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
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

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:

```
cluster::*> network interface show -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            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
8 entries were displayed.
```

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_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
```

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.

```
CL1# 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      Eth1/41(D)   Eth1/42(D)   Eth1/43(D)
                                     Eth1/44(D)   Eth1/45(P)   Eth1/46(P)
                                     Eth1/47(P)   Eth1/48(P)
```

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.

```
cluster::*> network interface show -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            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.
```

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      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
Port      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 -        -
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_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)
```

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` *`source-node-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:

```
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            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 entries were displayed.

----- ------- ----
```

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)# exit
C2#
```

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:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
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.
```

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     Po1(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      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
Port      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 -        -
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:

```
cluster::*> network interface show -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            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.
```

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_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)
```

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:

    ◦ `network device-discovery show`

    ◦ `network port show -role cluster`

    ◦ `network interface show -role cluster`

    ◦ `system cluster-switch show`

```
cluster::> network device-discovery show
            Local  Discovered
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 displayed.
```

```
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  -
-
e0c       Cluster      Cluster         up   9000 auto/10000  -
-
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 -
-
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      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
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
```

```
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

```
cluster::*> network interface show -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
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
12 entries were displayed.
```

```
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)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                      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)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

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. 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
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 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
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
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       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

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 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
------------------------------------------------------------------------
--------
1     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
ID
C2                 Eth1/31        174    R S I s     N3K-C3232C  Eth1/31
C2                 Eth1/32        174    R S I s     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    R S I s     N3K-C3232C  Eth1/31
C1                 Eth1/32        178    R S I s     N3K-C3232C  Eth1/32
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
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 interface show -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            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 were displayed.
```

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      Cluster          up   9000 auto/40000  -

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.

```
cluster::*> network interface show -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
            n1_clus2   up/up      10.10.0.2/24       n1            e4e
true
            n2_clus1   up/up      10.10.0.3/24       n2            e4a
true
            n2_clus2   up/up      10.10.0.4/24       n2            e4e
true
4 entries were displayed.
```

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`

```
cluster::*> network interface show -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
            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 were displayed.
```

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.

```
cluster::*> network interface show -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
            n1_clus2   up/up      10.10.0.2/24       n1            e4e
true
            n2_clus1   up/up      10.10.0.3/24       n2            e4a
true
            n2_clus2   up/up      10.10.0.4/24       n2            e4e
true
4 entries were displayed.
```

31. Verify that all of the cluster interconnect ports are in the `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::*> network device-discovery show
            Local  Discovered
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: 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     10.10.1.102
NX3232CV
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 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        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)
```

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
```

```
cluster::> network device-discovery show
            Local  Discovered
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

n4         /cdp
            e4a    CL1                 Ethernet1/8      N3K-C3232C
            e4e    CL2                 Ethernet1/8      N3K-C3232C

12 entries were displayed
```

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
--------- ------------ ---------------- ---- ---- -----------
------------
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
Port      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 -
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

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: n4

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  -

12 entries were displayed.
```

b. Display information about the logical interfaces (LIFs):

`network interface show -role cluster`

```
cluster::*> network interface show -role cluster
             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
e0a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e0e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e0a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e0e     true

12 entries were displayed.
```

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
--------------------------- ------------------ ----------------
---------------
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)I6(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

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`

```
cluster::*> network interface show -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            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
            n3_clus1   up/up      10.10.0.9/24       n3            e4a
true
            n3_clus2   up/up      10.10.0.10/24      n3            e4a
false
            n4_clus1   up/up      10.10.0.11/24      n4            e4a
true
            n4_clus2   up/up      10.10.0.12/24      n4            e4a
false
12 entries were displayed.
```

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        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
Cluster n3_clus1 n4        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 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)
8   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:

```
CL1# 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)
```

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.

```
Ports Eth1/31 and Eth1/32 should indicate (P), which means that both ISL
ports are up in the port-channel.
Example
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)
```

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.

```
cluster::*> network interface show -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            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
12 entries were displayed.
```

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          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
Port      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 -
e0d       Cluster      Cluster          up   9000  auto/10000 -        -
Node: n3

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: n4

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  -
        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        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
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)
```

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 show`
    - `network port show -role cluster`
    - `network interface show -role cluster`
    - `system cluster-switch show`

```
cluster::> network device-discovery show
            Local  Discovered
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 displayed.
```

```
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  -
e0c       Cluster      Cluster          up   9000 auto/10000  -
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 -
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      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
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
Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -

12 entries were displayed.
```

```
cluster::*> network interface show -role cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            nm1_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
 12 entries were displayed.
```

```
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)I6(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: 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    10.10.1.103      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
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::*> 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      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
```

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       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/lldp
            e3a    S1                        Ethernet1/2       -
            e4a    node1                     e4a               -
            e4e    node1                     e4e               -
```

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           e3a
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::*> 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
```

9. 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
            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/lldp
            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`

```
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  Ethernet1/5 NS2
3.20  2  Ethernet1/6 S1
3.20  3  Ethernet1/6 NS2
3.30  0  Ethernet1/7 S1
3.20  1  Ethernet1/7 NS2
3.30  2  Ethernet1/8 S1
3.20  3  Ethernet1/8 NS2
```

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

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 that the storage switches are available:
`system switch ethernet show`

```
storage::*> system switch ethernet show
Switch                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
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::*> 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:
   `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
% Total    % Received % Xferd  Average  Speed   Time    Time     Time
Current
                               Dload    Upload  Total   Spent    Left
Speed
  100        3254       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 `Nexus_3232C_RCF_v1.6-Storage.txt` 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
------  --------  --------------  ------------  ------
     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                                  9.3(3)
9.3(4)           yes
     1        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
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 08.38
 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                      Type               Address          Model
--------------------------- ------------------ ----------------
---------------
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::*> 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 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.
```

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).

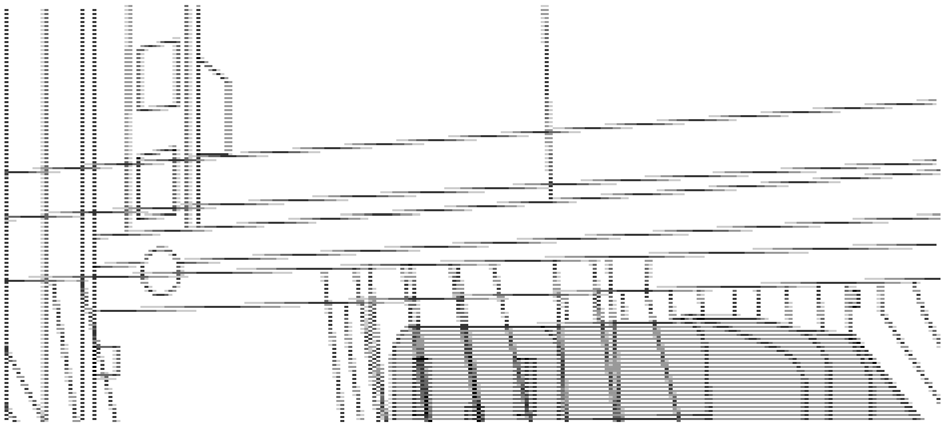
   The NetApp pass-through panel kit contains the following hardware:

   - 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.

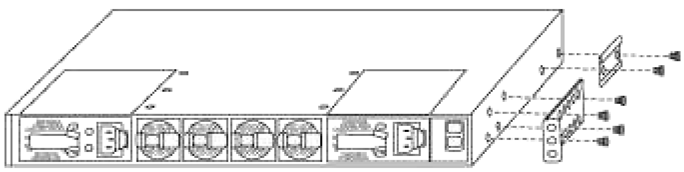
d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



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.

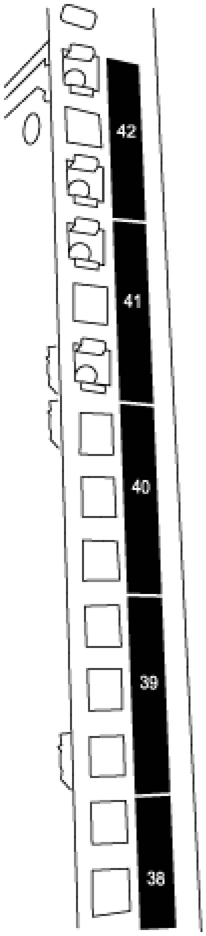
   

   b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.

   c. Install the rear rack-mount bracket on the switch chassis.

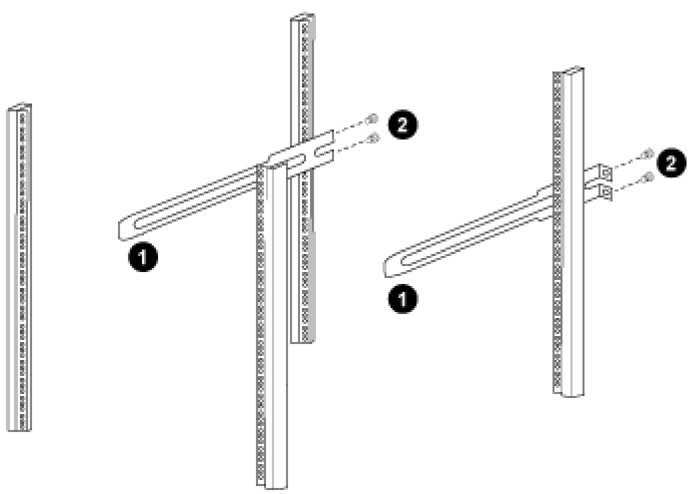
   d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.

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.



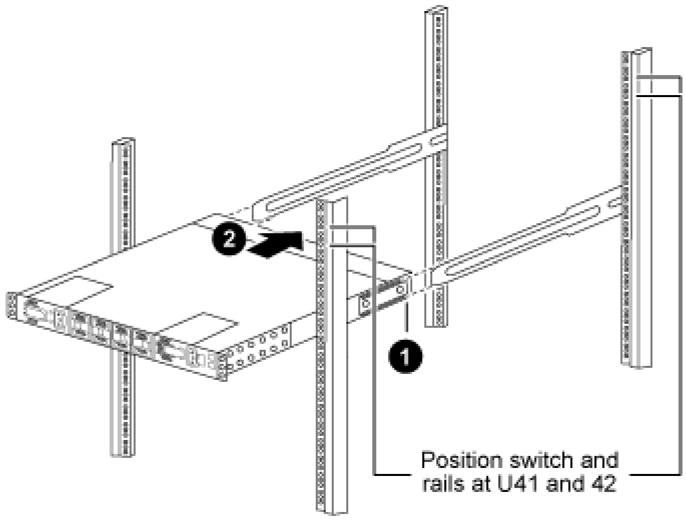
      i. As you gently slide the slider rail, align it to the screw holes in the rack.
      ii. Tighten the screws of the slider rails to the cabinet posts.
   b. Repeat step 4a for the right side rear post.

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.

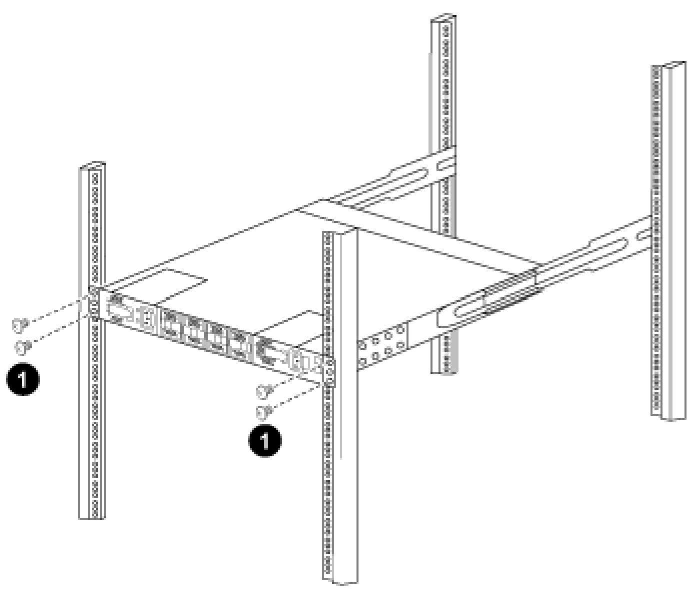
a. Position the back of the switch at RU41.



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 *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.
Cisco Nexus 3232C in a NetApp system cabinet	See the *Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet* guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the *Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet* 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 set-privilege 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 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 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 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 **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::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------- --------
cluster1-02/cdp
            e0a    cs1                       Eth1/2            N9K-
C9336C
            e0b    cs2                       Eth1/2            N9K-
C9336C
cluster1-01/cdp
            e0a    cs1                       Eth1/1            N9K-
C9336C
            e0b    cs2                       Eth1/1            N9K-
C9336C

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`

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02
                                                  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: 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 -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   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 were 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` 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.

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: 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 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
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 08.38
  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
------- --------- ----------------------------------------
------------------- ------------
  1      nxos     9.3(4)                                   9.3(5)
yes
  1      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`

```
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 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
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
------  ------------------ ----------------- --------- -----
     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           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.
```

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
GEM  FPGA                        0x2
GEM  FPGA                        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.
> - Before you perform this procedure make sure that you have a current backup of the switch configuration.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches: `network device-discovery show`

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------  --------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C
cluster1::*>
```

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/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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
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 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: cluster1-04

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
cluster1::*>
```

b. Verify that all the cluster interfaces (LIFs) are on the home port: `network interface show -role` cluster

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
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  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
            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 entries were displayed.
cluster1::*>
```

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`

```
cluster1::*> network interface show -role cluster
            Logical          Status     Network            Current
Current Is
Vserver     Interface        Admin/Oper Address/Mask       Node
Port    Home
----------- ---------------- ---------- ------------------
------------- ------- ----
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     false
            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
e0a     false
            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
e0a     false
            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     false
8 entries were displayed.
cluster1::*>
```

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 displayed.
cluster1::*>
```

7. If you have not already done so, save the current switch configuration by copying the output of the following command to a log file:

```
show running-config
```

8. 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.

9. 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)...
   ```

10. 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
    ```

11. 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
g mode:
* no interface breakout module 1 port <range> map 10g-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
*
****************************************************************************
******
```

12. 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.

13. 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.

```
cs2# copy running-config startup-config
[########################################] 100% Copy complete
```

14. 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
```

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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
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      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: cluster1-03

Ignore
                                                  Speed(Mbps) Health
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
healthy false

Node: cluster1-04

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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::*> network device-discovery show -protocol cdp
Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
```

```
--------
cluster1-01/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
cluster1-04/cdp
            e0a    cs1                      Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                      Ethernet1/1/2     N9K-
C9336C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ---------------- -----
cs1                         cluster-network    10.233.205.90    NX9-
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    NX9-
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
```

```
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.
```

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`

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     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
            cluster1-02_clus1  up/up      169.254.3.8/23     cluster1-02
e0d     false
            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
e0b     false
            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
e0b     true
8 entries were displayed.
cluster1::*>
```

18. 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 displayed.
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
.
.
Eth1/1/1      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`

```
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      Eth1/35(P)        Eth1/36(P)
cs1#
```

24. Verify that the cluster LIFs have reverted to their home port: `network interface show -role cluster`

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
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
e0b     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
e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23     cluster1-04
e0b     true
8 entries were displayed.
cluster1::*>
```

25. 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 displayed.
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 from a Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch

Migrate from an older 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 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 an older 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.

Before you begin

The following conditions must exist before replacing an older Cisco Nexus cluster switch with a Cisco Nexus 9336C-FX2 cluster switch:

- The cluster must be fully functioning (there should be no errors in the logs or similar issues).
- Initial customization of the Cisco Nexus 9336C-FX2 switches must be completed. So that the:
  - 9336C-FX2 switches are running the latest recommended version of software
  - Reference Configuration Files (RCFs) have been applied to the switches
  - Any site customization, such as DNS, NTP, SMTP, SNMP, and SSH must be configured on the new switches.
- You must have consulted the switch compatibility table on the Cisco Ethernet Switches page for the supported ONTAP, NX-OS, and RCF 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 on Nexus 9000 Series Switches.

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 the different releases of ONTAP.

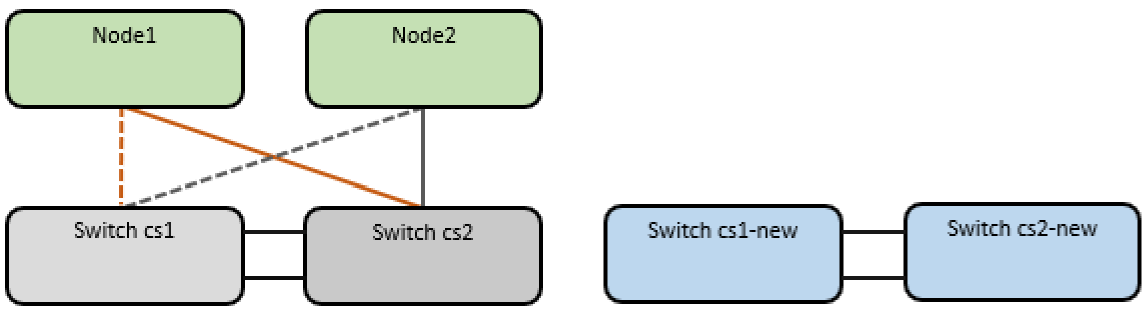
The examples in this procedure use the following switch and node nomenclature:

- The names of the existing two Cisco switches are **cs1** and **cs2**

- The new Nexus 9336C-FX2 cluster switches are **cs1-new** and **cs2-new**.
- The node names are **node1** and **node2**.
- The cluster LIF names are **node1_clus1** and **node1_clus2** for node 1, and **node2_clus1** and **node2_clus2** for node 2.
- The **cluster1::>*** prompt indicates the name of the cluster.

> The procedure requires the use of both ONTAP commands and Nexus 9000 Series Switches commands; ONTAP commands are used, unless otherwise indicated.

Initial switch setup



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. On the new switches, confirm that the ISL is cabled and healthy between the switches cs1-new and cs2-new: `show port-channel summary`

```
cs1-new# 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)

cs2-new# 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)
```

4. Display the cluster ports on each node that are connected to the existing cluster switches: `network device-discovery show`

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e0a    cs1                       Ethernet1/1        N5K-
C5596UP
            e0b    cs2                       Ethernet1/2        N5K-
C5596UP
node2      /cdp
            e0a    cs1                       Ethernet1/1        N5K-
C5596UP
            e0b    cs2                       Ethernet1/2        N5K-
C5596UP
```

5. Determine the administrative or operational status for each cluster port.
   a. Verify that all the cluster ports are up with a healthy status: `network port show -ipspace Cluster`

```
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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

b. Verify that all the cluster interfaces (LIFs) are on their home ports: `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
e0b     true
```

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    10.233.205.92    N5K-
C5596UP
      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   N5K-
C5596UP
      Serial Number: FOXXXXXXXGD
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(4)
     Version Source: CDP
```

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
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 -vserver Cluster`

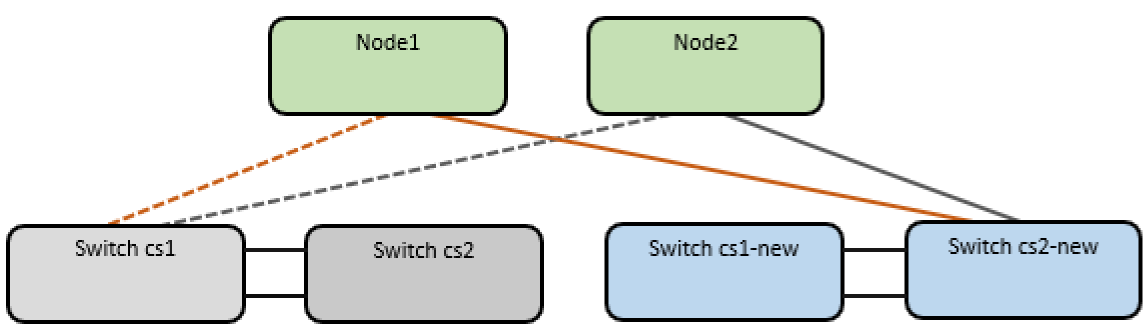
```
cluster1::*> network interface show -vserver Cluster
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node       Port
Home
----------- ------------- ---------- ------------------ ----------
------- ----
Cluster
            node1_clus1   up/up      169.254.3.4/16     node1      e0a
true
            node1_clus2   up/up      169.254.3.5/16     node1      e0a
false
            node2_clus1   up/up      169.254.3.8/16     node2      e0a
true
            node2_clus2   up/up      169.254.3.9/16     node2      e0a
false
```

9. Verify that the cluster is healthy: `cluster show`

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

10. Move all cluster node connections from the old cs2 switch to the new cs2-new switch.

Cluster node connections moved to the cs2-new switch



11. Confirm the health of the network connections moved to cs2-new: `network port show -ipspace Cluster`

```
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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

All cluster ports that were moved should be up.

12. Check neighbor information on the cluster ports:
`network device-discovery show -protocol cdp`

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface      Platform
----------- ------ ------------------------- -------------
--------------
node1      /cdp
            e0a    cs1                       Ethernet1/1    N5K-C5596UP
            e0b    cs2-new                   Ethernet1/1/1  N9K-C9336C-
FX2

node2      /cdp
            e0a    cs1                       Ethernet1/2    N5K-C5596UP
            e0b    cs2-new                   Ethernet1/1/2  N9K-C9336C-
FX2
```

Verify that the moved cluster ports see the cs2-new switch as the neighbor.

13. Confirm the switch port connections from switch cs2-new's perspective:

```
cs2-new# show interface brief
cs2-new# show cdp neighbors
```

14. 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 7.

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

All cluster LIFs will move to the cs2-new switch.

15. Verify that the cluster LIFs have migrated to the ports hosted on switch cs2-new. This might take a few seconds: `network interface show -vserver Cluster`

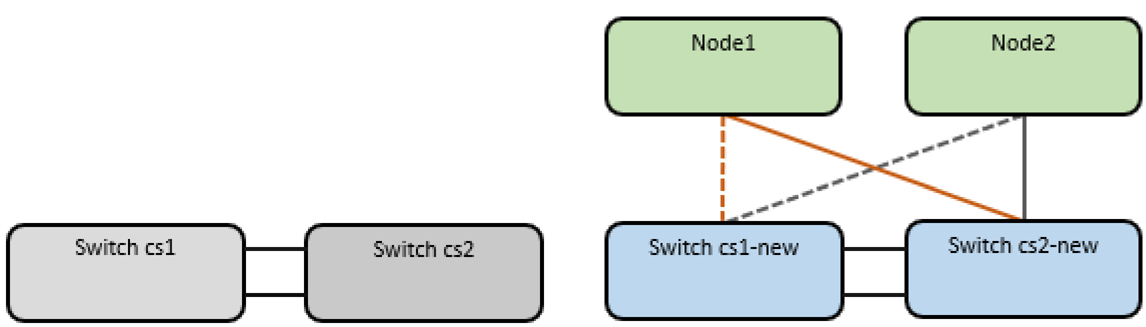
```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interfac     Admin/Oper Address/Mask       Node         Port
Home
----------- ------------ ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.3.4/16     node1        e0b
false
            node1_clus2  up/up      169.254.3.5/16     node1        e0b
true
            node2_clus1  up/up      169.254.3.8/16     node2        e0b
false
            node2_clus2  up/up      169.254.3.9/16     node2        e0b
true
```

16. Verify that the cluster is healthy: `cluster show`

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

17. Move the connections from cs1 to the new cs1-new switch.

Cluster node connections moved to the cs1-new switch



18. Confirm the health of the network connections moved to cs1-new: `network port show -ipspace Cluster`

```
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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

All cluster ports that were moved should be up.

19. Check neighbor information on the cluster ports: `network device-discovery show`

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface       Platform
----------- ------ ------------------------- --------------
--------------
node1      /cdp
            e0a    cs1-new                   Ethernet1/1/1   N9K-C9336C-
FX2
            e0b    cs2-new                   Ethernet1/1/2   N9K-C9336C-
FX2

node2      /cdp
            e0a    cs1-new                   Ethernet1/1/1   N9K-C9336C-
FX2
            e0b    cs2-new                   Ethernet1/1/2   N9K-C9336C-
FX2
```

Verify that the moved cluster ports see the cs1-new switch as the neighbor.

20. Confirm the switch port connections from switch cs1-new's perspective:

```
cs1-new# show interface brief
cs1-new# show cdp neighbors
```

21. Verify that the ISL between cs1-new and cs2-new is still operational: `show port-channel summary`

```
cs1-new# 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)

cs2-new# 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)
```

22. Enable auto-revert on the cluster LIFs.

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

23. Verify that the cluster LIFs have reverted to their home ports (this might take a minute): `network interface show -vserver Cluster`

    If the cluster LIFs have not reverted to their home port, manually revert them: `network interface revert -vserver Cluster -lif *`

24. Verify that the cluster is healthy: `cluster show`
25. Ping the remote cluster interfaces to verify connectivity: `cluster ping-cluster -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)
```

26. Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files.

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`

NOTE: You will need the password for the **admin** user on the switches.

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-new
cs2-new

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1-new
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: <password of switch's admin user>
Enter the password again: <password of switch's admin user>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2-new
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: <password of switch's admin user>
Enter the password again: <password of switch's admin user>
```

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::*>
```

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

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`

NOTE: You will need the password for the **admin** user on the switches.

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-new
cs2-new

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1-new
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: <password of switch's admin user>
Enter the password again: <password of switch's admin user>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2-new
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: <password of switch's admin user>
Enter the password again: <password of switch's admin user>
```

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::*>
```

NOTE: 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`

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.

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:

```
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:

```
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      Eth1/35(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)
```

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
ID
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     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 port show -ipspace Cluster

Node: node1

                                                  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: 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`

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

```
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.
```

8. 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_clus2   true

4 entries were displayed.
```

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 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.
```

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:

```
cluster1::*> cluster show

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 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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
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:

```
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    H           FAS2980       e0a
node2              Eth1/2         133    H           FAS2980       e0a
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     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         133    H           FAS2980       e0b
node2              Eth1/2         133    H           FAS2980       e0b
cs1                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        175    R S I s     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`

```
cluster1::*> network device-discovery show -protocol cdp
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.
```

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:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                true    true          false
```

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: 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.

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: 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.

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)

---- System Admin Account Setup ----
```

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: 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.

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: 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 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
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 08.38
  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
------- --------- ----------------------------------------
------------------- ------------
  1      nxos     9.3(4)                                  9.3(5)
yes
  1      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`

```
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 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
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
------  ------------------ ----------------- --------- -----
     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           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.
```

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
GEM  FPGA                        0x2
GEM  FPGA                        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.
> - Before performing this procedure, make sure that you have a current backup of the switch configuration.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches: `network device-discovery show`

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------  --------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C
cluster1::*>
```

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/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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
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 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: cluster1-04

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
cluster1::*>
```

b. Verify that all the cluster interfaces (LIFs) are on the home port: `network interface show -role` cluster

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network           Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
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  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
            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 entries were displayed.
cluster1::*>
```

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 ports have migrated to the ports hosted on cluster switch cs1. This might take a few seconds.`network interface show -role cluster`

```
cluster1::*> network interface show -role cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------- ------- ----
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     false
            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
e0a     false
            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
e0a     false
            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     false
8 entries were displayed.
cluster1::*>
```

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 displayed.
cluster1::*>
```

7. If you have not already done so, save the current switch configuration by copying the output of the following command to a log file:

```
show running-config
```

8. 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.
9. 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)...
```

10. 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
```

11. 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
g mode:
* no interface breakout module 1 port <range> map 10g-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
*
******************************************************************************
******
```

12. 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.

13. 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.

```
cs2# copy running-config startup-config
[########################################] 100% Copy complete
```

14. 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
```

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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
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      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: cluster1-03

Ignore
                                                  Speed(Mbps) Health
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
healthy false

Node: cluster1-04

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
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::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
```

```
--------
cluster1-01/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
cluster1-04/cdp
            e0a    cs1                      Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                      Ethernet1/1/2     N9K-
C9336C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ---------------- -----
cs1                         cluster-network    10.233.205.90    NX9-
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    NX9-
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
```

```
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.
```

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`

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     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
            cluster1-02_clus1  up/up      169.254.3.8/23     cluster1-02
e0d     false
            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
e0b     false
            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
e0b     true
8 entries were displayed.
cluster1::*>
```

18. 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 displayed.
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
.
.
Eth1/1/1       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`

```
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      Eth1/35(P)        Eth1/36(P)
cs1#
```

24. Verify that the cluster LIFs have reverted to their home port: `network interface show -role cluster`

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
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
e0b     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
e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23     cluster1-04
e0b     true
8 entries were displayed.
cluster1::*>
```

25. 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 displayed.
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)
```

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:

```
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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
4 entries were displayed.



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.
```

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2            N9K-C9336C
            e0b    cs2                       Eth1/2            N9K-C9336C
node1      /cdp
            e0a    cs1                       Eth1/1            N9K-C9336C
            e0b    cs2                       Eth1/1            N9K-C9336C
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    H           FAS2980       e0a
node2              Eth1/2         145    H           FAS2980       e0a
cs2                Eth1/35        176    R S I s     N9K-C9336C    Eth1/35
cs2(FDO220329V5)   Eth1/36        176    R S I s     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         139    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1                Eth1/35        178    R S I s     N9K-C9336C    Eth1/35
cs1                Eth1/36        178    R S I s     N9K-C9336C    Eth1/36

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`

```
cluster1::> network interface show -vserver Cluster -fields auto-revert

             Logical
Vserver      Interface     Auto-revert
------------ ------------- -------------
Cluster      node1_clus1   true
Cluster      node1_clus2   true
Cluster      node2_clus1   true
Cluster      node2_clus2   true

4 entries were displayed.
```

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

cs1(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
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member       Ports
      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:

```
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       Cluster      Cluster          up   9000  auto/10000  healthy
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
e0b       Cluster      Cluster          up   9000  auto/auto   -
false

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 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 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      e0a
false

4 entries were 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`

```
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       Cluster     Cluster           up    9000  auto/10000  healthy
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
e0b       Cluster      Cluster          up    9000  auto/10000  healthy
false

4 entries were displayed.
```

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 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`

```
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       Cluster     Cluster          up   9000  auto/10000  healthy
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
e0b       Cluster      Cluster          up   9000 auto/10000  healthy
false

4 entries were displayed.


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.

cluster1::> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C9336C
            e0b    newcs2                    0/2               N9K-
C9336C
```

```
node1      /cdp
            e0a    cs1                         0/1               N9K-
C9336C
            e0b    newcs2                      0/1               N9K-
C9336C

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    H           FAS2980       e0a
node2                Eth1/2         145    H           FAS2980       e0a
newcs2               Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
newcs2               Eth1/36        176    R S I s     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         139    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1                Eth1/35        178    R S I s     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: 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.

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

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.

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 -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   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                     e4e         AFF-A700
node1/lldp
           e3a   S1                        Ethernet1/1 -
           e4a   node2                     e4a         -
           e4e   node2                     e4e         -
node2/cdp
           e3a   S1                        Ethernet1/2 NX9336C
           e4a   node1                     e4a         AFF-A700
           e4e   node1                     e4e         AFF-A700
node2/lldp
           e3a   S1                        Ethernet1/2 -
           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             e3a
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   -             -
storage::*>
```

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::*> 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   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::*>
```

9. 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
          e3a  S1                         Ethernet1/1 NX9336C
          e4a  node2                      e4a         AFF-A700
          e4e  node2                      e4e         AFF-A700
          e7b   NS2                       Ethernet1/1 NX9336C
node1/lldp
          e3a  S1                         Ethernet1/1 -
          e4a  node2                      e4a         -
          e4e  node2                      e4e         -
          e7b  NS2                        Ethernet1/1 -
node2/cdp
          e3a  S1                         Ethernet1/2 NX9336C
          e4a  node1                      e4a         AFF-A700
          e4e  node1                      e4e         AFF-A700
          e7b  NS2                        Ethernet1/2 NX9336C
node2/lldp
          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    1     Ethernet1/5     NS2
3.20    2     Ethernet1/6     S1
3.20    3     Ethernet1/6     NS2
3.30    0     Ethernet1/7     S1
3.20    1     Ethernet1/7     NS2
3.30    2     Ethernet1/8     S1
3.20    3     Ethernet1/8     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 configuration. If you want to build ONTAP clusters 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
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

1. Rack the switches, controllers and NS224 NVMe storage shelves. 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, controllers and NS224 NVMe storage shelves.
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 A700s 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.

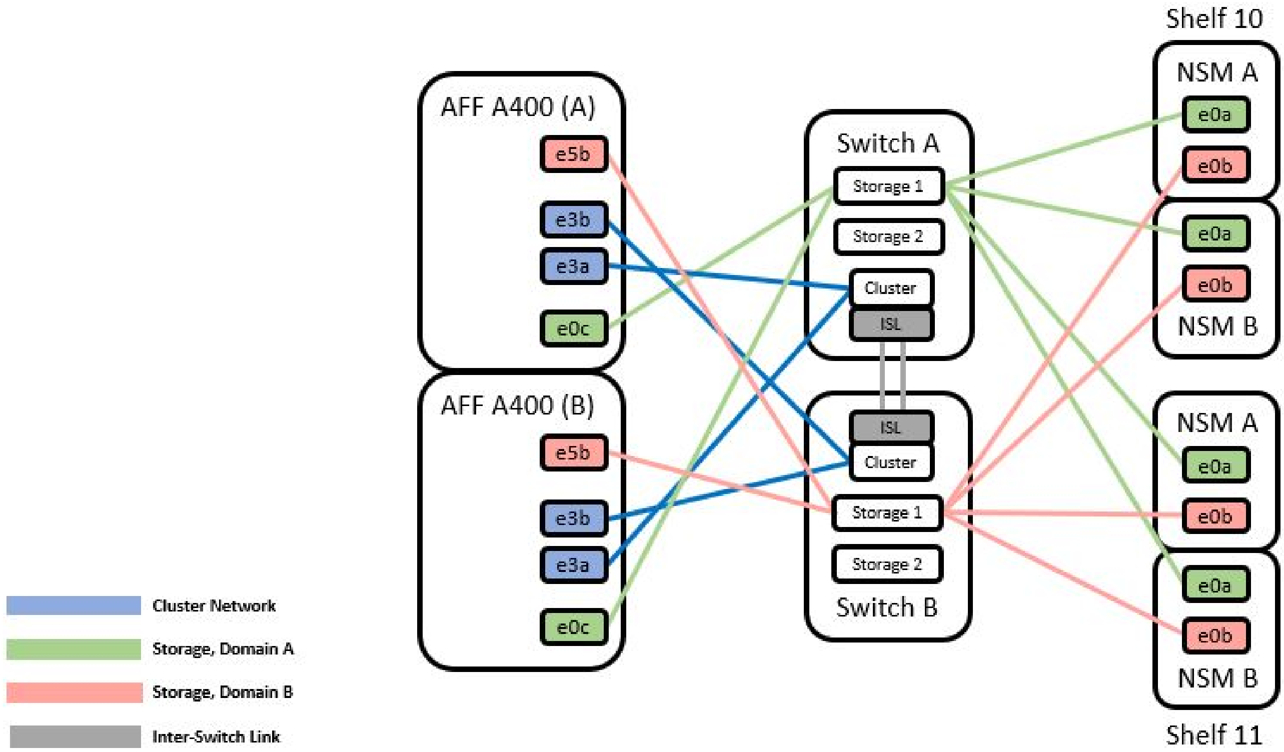
To set up the Cisco Nexus 9336C-FX2 shared switches, see the Cisco Nexus 9000 Series Switches Support page.

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

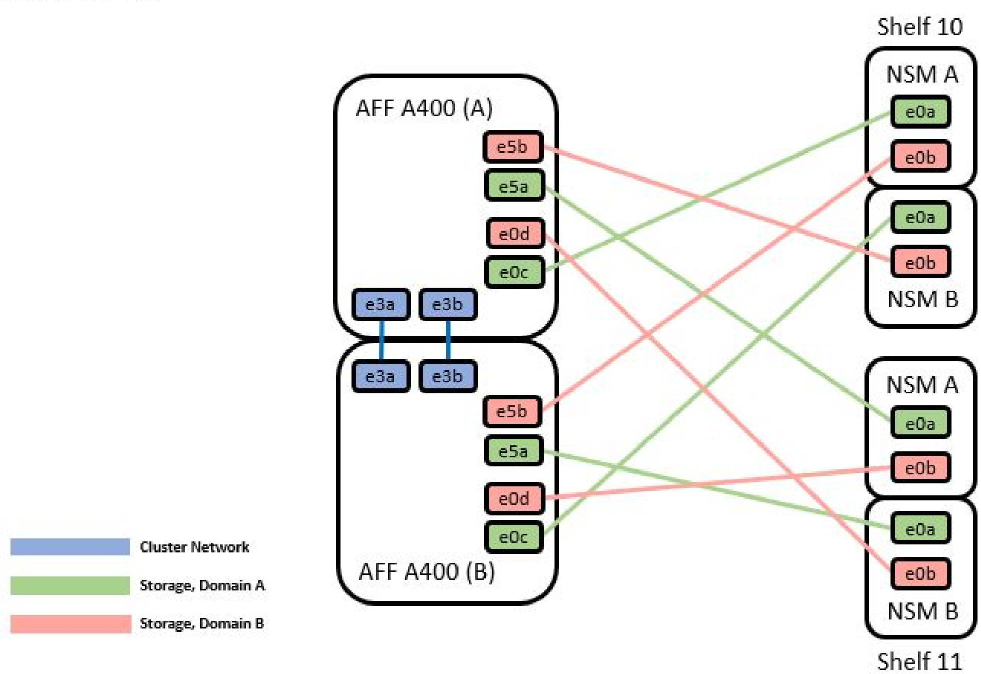
You can use the following cabling images to complete the cabling between the controllers and the switches. If you want to cable NS224 storage as switch-attached, follow the switch-attached diagram:

Switch Attached



If you want to cable NS224 storage as direct-attached instead of using the shared switch storage ports, follow the direct-attached diagram:

Direct Attached



	Port	Node
Path_A	e0c	Node_A
		Node_B
	e5a	Node_A
		Node_B
Path_B	e5b	Node_A
		Node_B
	e0d	Node_A
		Node_B

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.
> - Before you perform this procedure, make sure that you have a current backup of the switch configuration.

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=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`

```
cluster1:: network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------- --------
cluster1-02/cdp
            e3a    cs1                       Eth1/2            N9K-
C9336C
            e3b    cs2                       Eth1/2            N9K-
C9336C
cluster1-01/cdp
            e3a    cs1                       Eth1/1            N9K-
C9336C
            e3b    cs2                       Eth1/1            N9K-
C9336C
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`

```
cluster1::*> network port show -ipspace Cluster
Node: cluster1-02
                                                      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: cluster1-01
                                                      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 entries were displayed.
```

b. Display information about the LIFs:
`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
        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
4 entries were 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     e3a
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`

```
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. 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|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.
   ```

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:
`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 08.38
  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
------- --------- --------------------------------------
------------------- ------------
  1      nxos     9.3(4)                                9.3(5)
yes
  1      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
```

```
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 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
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
------  -------------- ------------ ----------- -------
     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           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.
```

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
GEM  FPGA                        0x2
GEM  FPGA                        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.
> - Before you perform this procedure, make sure that you have a current backup of the switch configuration.

Steps

1. Display the cluster ports on each node that are connected to the cluster switches:
   `network device-discovery show`

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------  --------
cluster1-01/cdp
            e3a    cs1                       Ethernet1/7       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster1-02/cdp
            e3a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster1-03/cdp
            e3a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e3b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/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`

```
cluster1::*> network port show -role cluster
Node: cluster1-01

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e3a       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
--------- ------------ ---------------- ---- ---- ----------- --------
------
e3a       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
--------- ------------ ---------------- ---- ---- ------------ --------
------
e3a       Cluster      Cluster          up   9000  auto/100000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/100000 healthy
false
Node: cluster1-04

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`

```
cluster1::*> network interface show -role cluster
        Logical            Status     Network         Current
Current Is
Vserver Interface          Admin/Oper Address/Mask    Node          Port
Home
------- ------------------ ---------- --------------- ------------
------- ----
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  e0d
true
        cluster1-02_clus1  up/up     169.254.3.8/23   cluster1-02  e3a
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  e3a
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  e3a
true
        cluster1-04_clus2  up/up     169.254.1.7/23   cluster1-04  e3b
true
8 entries were displayed.
cluster1::*>
```

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          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::*>
```

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`

```
cluster1::*> network interface show -role cluster
        Logical           Status     Network          Current
Current  Is
Vserver Interface         Admin/Oper Address/Mask     Node          Port
Home
------- ----------------- ---------- ---------------- -------------
------- ----
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 up/up     169.254.3.8/23   cluster1-02   e3a
true
        cluster1-02_clus2 up/up     169.254.3.9/23   cluster1-02   e3a
false
        cluster1-03_clus1 up/up     169.254.1.3/23   cluster1-03   e3a
true
        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
8 entries were displayed.
cluster1::*>
```

9. 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 displayed.
cluster1::*>
```

10. If you have not already done so, save the current switch configuration by copying the output of the following command to a log file:

```
show running-config
```

11. 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.

12. 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)...
    ```

13. 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
    ```

14. 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
* config mode:
* no interface breakout module 1 port <range> map 10g-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
*
**********************************************************************
***
```

15. 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.

16. 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
```

17. 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
```

18. 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
```

19. 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
------- --------- ---------------- ---- ---- ------------ --------
------
e3a     Cluster   Cluster          up   9000 auto/100000  healthy
false
e3b     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
------- --------- ---------------- ---- ----- ------------ --------
------
e3a    Cluster   Cluster          up   9000  auto/100000  healthy
false
e3b    Cluster   Cluster          up   9000  auto/100000  healthy
false

Node: cluster1-03

Ignore
                                              Speed(Mbps) Health
Health
Port   IPspace    Broadcast Domain Link MTU   Admin/Oper  Status
Status
------ ---------- ---------------- ---- ----- ----------- --------
------
e3a    Cluster    Cluster          up   9000  auto/100000 healthy
false
e0d    Cluster    Cluster          up   9000  auto/100000 healthy
false

Node: cluster1-04

Ignore
                                              Speed(Mbps) Health
Health
Port   IPspace    Broadcast Domain Link MTU   Admin/Oper  Status
Status
------ ---------- ---------------- ---- ----- ----------- --------
------
e3a    Cluster      Cluster        up   9000  auto/100000 healthy
false
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::*> network device-discovery show -protocol cdp
```

```
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e3a    cs1                       Ethernet1/7       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster01-2/cdp
            e3a    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
cluster1-04/cdp
            e3a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e3b    cs2                       Ethernet1/1/2     N9K-
C9336C
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ---------------- -----
cs1                         cluster-network    10.233.205.90    NX9-
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    NX9-
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
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.
```

20. 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
```

21. 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`

```
cluster1::*> network interface show -role cluster
        Logical            Status      Network         Current
Current Is
Vserver 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
        cluster1-02_clus1  up/up       169.254.3.8/23   cluster1-02
e0d  false
        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  false
        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  false
        cluster1-04_clus2  up/up       169.254.1.7/23   cluster1-04
e3b   true
8 entries were displayed.
cluster1::*>
```

22. 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 displayed.
cluster1::*>
```

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

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

25. 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
```

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

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      1       eth  access up      none                      100G(D)
--
Eth1/1/2      1       eth  access up      none                      100G(D)
--
Eth1/7        1       eth  trunk  up      none                      100G(D)
--
Eth1/8        1       eth  trunk  up      none                      100G(D)
--
.
.
```

27. Verify that the ISL between cs1 and cs2 is functional:
`show port-channel summary`

```
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      Eth1/35(P)        Eth1/36(P)
cs1#
```

28. Verify that the cluster LIFs have reverted to their home port:
`network interface show -role cluster`

```
cluster1::*> network interface show -role cluster
        Logical            Status     Network           Current
Current Is
Vserver Interface          Admin/Oper Address/Mask      Node        Port
Home
------- ------------------ ---------- ----------------- -----------
------- ----
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
true
8 entries were displayed.
cluster1::*>
```

29. 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 displayed.
cluster1::*>
```

30. 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.
> - Before you perform this procedure, make sure that you have a current backup of the switch configuration.

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
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::*>
```

3. Verify that the node ports are healthy and operational:
`storage port show -port-type ENET`

```
storage::*> 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:
`system health alert show -instance`

```
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        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                                   9.3(3)          9.3(4)
yes
 1     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.
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
   Dload     Upload  Total  Spent    Left
Speed
 100    3254          100     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`

```
storage::*> 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
 100    5143          100     5143      0       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 motd` 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
*Port    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 25g-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 port
* 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:

```
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:

```
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      Eth1/35(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)
```

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
ID
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     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 port show -ipspace Cluster

Node: node1
                                                      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: node2
                                                      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 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.

```
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         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 were displayed.
```

8. 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_clus2   true
4 entries were displayed.
```

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**:

```
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       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 were displayed.
```

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:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
2 entries were displayed.
```

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 port show -ipspace Cluster

Node: node1

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: node2

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
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:

```
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      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 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    H           AFFA400       e3a
node2              Eth1/2         133    H           AFFA400       e3a
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     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         133    H           AFFA400       e3b
node2              Eth1/2         133    H           AFFA400       e3b
cs1                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        175    R S I s     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`

```
cluster1::*> network device-discovery show -protocol cdp
Node/       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
4 entries were displayed.
```

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                    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::*>
```

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:

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

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::*> 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
```

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`

```
storage::*> 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            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::*> 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            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`

```
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::*>
```

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.
  - 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

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.

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`

```
cluster1::*> network port show -role cluster
Node: node1

Ignore
                                             Speed(Mbps)  Health
Health
Port    IPspace   Broadcast Domain Link MTU  Admin/Ope    Status
Status
------- --------- ---------------- ---- ---- ------------ --------
------
e3a     Cluster   Cluster          up   9000  auto/100000 healthy  false
e3b     Cluster   Cluster          up   9000  auto/100000 healthy  false

Node: node2

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
4 entries were displayed.
cluster1::*>
```

4. Verify that all the cluster interfaces (LIFs) are on the home port:
`network interface show -role cluster`

```
cluster1::*> network interface 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 entries were displayed.
cluster1::*>
```

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          Model
------------------------- ------------------ ---------------- ------
sh1                       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
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
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
          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
         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     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::*>
```

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`

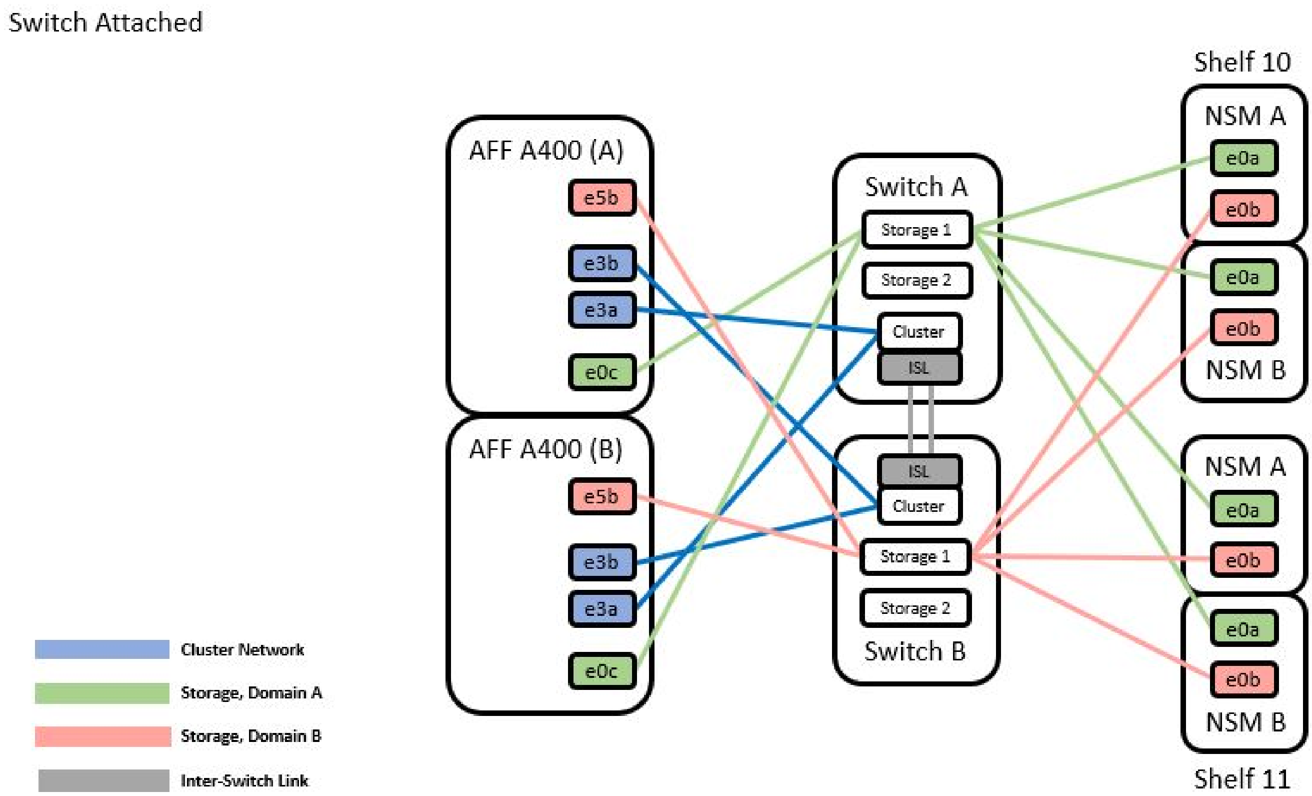
```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
node1                true    true          false
node2                true    true          false
2 entries were displayed.
cluster1::*>
```

Migrate from a switchless configuration 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



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-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 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
```

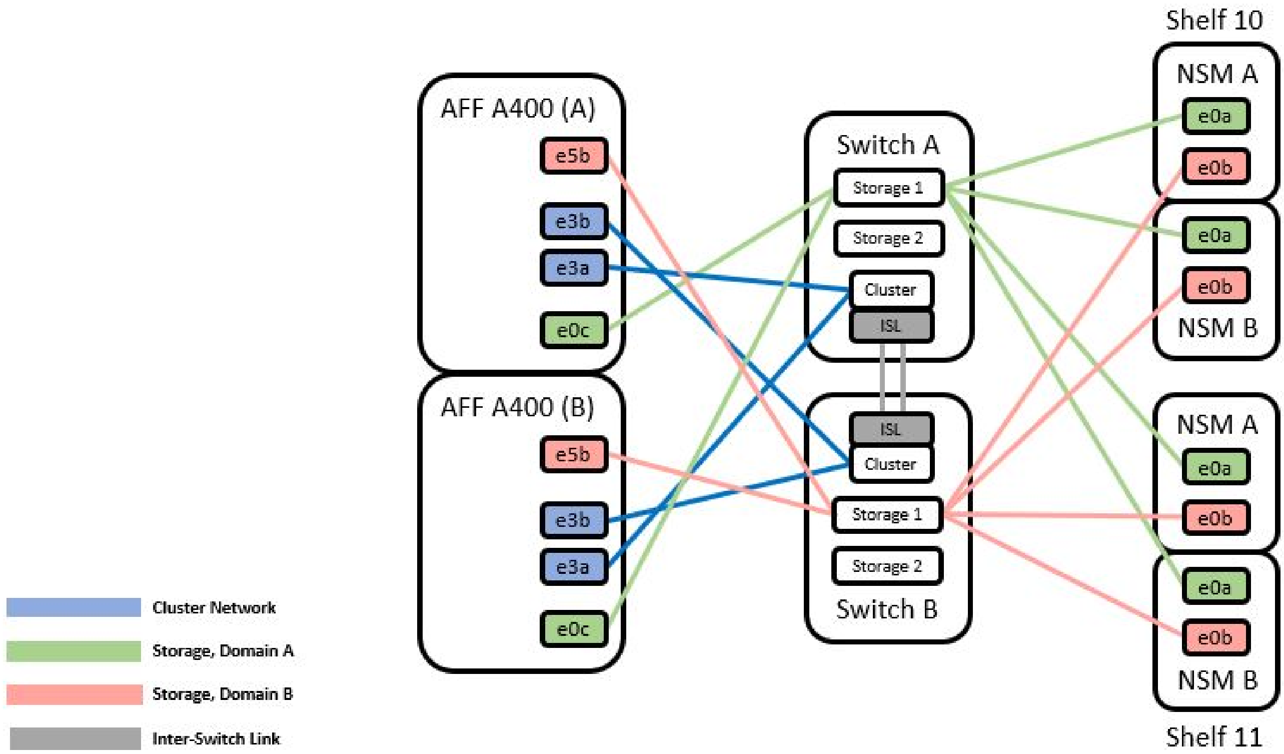
16. Convert HA pair 1 from a switchless cluster to a switched cluster. Use the cluster port assignments defined by the shared RCF. See Install NX-OS software and Reference Configuration Files (RCFs) for further details.
17. Verify that the switched networking configuration is valid:
`network port show`

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
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. 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`

```
storage::*> 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
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::*>
```

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:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

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: node2

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
4 entries were displayed.


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         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 were displayed.

cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e3a    sh1                       Eth1/2            N9K-
C9336C
            e3b    sh2                       Eth1/2            N9K-
C9336C

node1      /cdp
            e3a    sh1                       Eth1/1            N9K-
C9336C
            e3b    sh2                       Eth1/1            N9K-
C9336C
4 entries were displayed.

sh1# 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    H           FAS2980       e3a
node2                Eth1/2         145    H           FAS2980       e3a
sh2                  Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
sh2 (FDO220329V5)     Eth1/36       176    R S I s     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    H           FAS2980       eb
node2                Eth1/2         124    H           FAS2980       eb
sh1                  Eth1/35        178    R S I s     N9K-C9336C
Eth1/35
sh1                  Eth1/36        178    R S I s     N9K-C9336C
Eth1/36
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.

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`

```
cluster1::> network interface show -vserver Cluster -fields auto-revert
             Logical
Vserver      Interface     Auto-revert
------------ ------------- -------------
Cluster      node1_clus1   true
Cluster      node1_clus2   true
Cluster      node2_clus1   true
Cluster      node2_clus2   true
4 entries were displayed.
```

5. Verify that all the cluster LIFs can communicate:
`cluster ping-cluster <node name>`

```
cluster1::*> cluster ping-cluster 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)
```

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
```

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
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)

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 port show -ipspace Cluster

Node: node1

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: node2

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/auto    -
false
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 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      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 were 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`

```
cluster1::*> network port show -ipspace Cluster

Node node1
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: node2

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
4 entries were displayed.
```

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`

```
cluster1::*> network port show -ipspace Cluster

Node: node1

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: node2
```

```
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
4 entries were displayed.

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         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 were displayed.

cluster1::> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e3a    sh1    0/2               N9K-C9336C
            e3b    newsh2                    0/2               N9K-
C9336C
node1      /cdp
            e3a    sh1                       0/1               N9K-
C9336C
            e3b    newsh2                    0/1               N9K-
C9336C
```

```
4 entries were displayed.

sh1# 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    H           FAS2980       e3a
node2                Eth1/2         145    H           FAS2980       e3a
newsh2               Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
newsh2               Eth1/36        176    R S I s     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    H           FAS2980       e3b
node2              Eth1/2         124    H           FAS2980       eb
sh1                Eth1/35        178    R S I s     N9K-C9336C
Eth1/35
sh1                Eth1/36        178    R S I s     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`

```
storage::*> 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`

```
cluster1::*> storage shelf port show -fields remote-device,remote-port
shelf id remote-port  remote-device
----- -- ------------ ----------------------------
3.20  0  Ethernet1/13 sh1
3.20  1  Ethernet1/13 newsh2
3.20  2  Ethernet1/14 sh1
3.20  3  Ethernet1/14 newsh2
3.30  0  Ethernet1/15 sh1
3.30  1  Ethernet1/15 newsh2
3.30  2  Ethernet1/16 sh1
3.30  3  Ethernet1/16 newsh2
8 entries were displayed.
```

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 *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.
Cisco Nexus 3232C in a NetApp system cabinet	See the *Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet* guide for instructions to install the switch in a NetApp cabinet.
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the *Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet* 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 *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 set-privilege 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	
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	
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**	
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.

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 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]: 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 FDO220329V5

  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`

```
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 FDO220329V5

  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.

```
cs2# show version 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# install epld bootflash:n9000-epld.9.2.2.img module 1
Compatibility check:
Module        Type         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                    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.
```

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
GEM FPGA                        0x2
GEM FPGA                        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] 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.

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=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`

```
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

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`

```
cluster1::*> network port show -ipspace 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

Node: node1
                                                  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 -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.
```

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     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)
```

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
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

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
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 FDO220329V5

  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`

```
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 FDO220329V5

  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.

```
cs2# show version 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# install epld bootflash:n9000-epld.9.2.2.img module 1
Compatibility check:
Module        Type         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                     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.
```

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
GEM FPGA                         0x2
GEM FPGA                         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] 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:

```
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)
```

   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      Eth1/65(P)   Eth1/66(P)
```

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
ID
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    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:

```
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(FDO220329KU)    Eth1/65        177    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)    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
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

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`

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

```
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.
```

8. 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_clus2   true

4 entries were displayed.
```

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:

```
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.
```

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:

```
cluster1::*> cluster show

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:

```
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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
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:

```
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    H          FAS2980       e0a
node2               Eth1/2         133    H          FAS2980       e0a
cs2(FDO220329V5)    Eth1/65        175    R S I s    N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s    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    H          FAS2980       e0b
node2               Eth1/2         133    H          FAS2980       e0b
cs1(FDO220329KU)
                    Eth1/65        175    R S I s    N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                    Eth1/66        175    R S I s    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
```

```
cluster1::*> 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

4 entries were displayed.
```

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:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                true    true          false
```

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. 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:

    `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.

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_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 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       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false

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
            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.
```

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`

```
cluster1::*> 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

4 entries were displayed.
```

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

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         124    H          FAS2750
e0a
node2               Eth1/2         124    H          FAS2750
e0a
c2(FOX2025GEFC)     Eth1/41        179    S I s      N5K-C5596UP
Eth1/41

c2(FOX2025GEFC)     Eth1/42        175    S I s      N5K-C5596UP
Eth1/42

c2(FOX2025GEFC)     Eth1/43        179    S I s      N5K-C5596UP
Eth1/43

c2(FOX2025GEFC)     Eth1/44        175    S I s      N5K-C5596UP
Eth1/44

c2(FOX2025GEFC)     Eth1/45        179    S I s      N5K-C5596UP
Eth1/45

c2(FOX2025GEFC)     Eth1/46        179    S I s      N5K-C5596UP
Eth1/46

c2(FOX2025GEFC)     Eth1/47        175    S I s      N5K-C5596UP
Eth1/47

c2(FOX2025GEFC)     Eth1/48        179    S I s      N5K-C5596UP
Eth1/48

Total entries displayed: 10


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
node1               Eth1/1         124    H          FAS2750
e0b
node2               Eth1/2         124    H          FAS2750
e0b
c1(FOX2025GEEX)     Eth1/41        175    S I s      N5K-C5596UP
Eth1/41

c1(FOX2025GEEX)     Eth1/42        175    S I s      N5K-C5596UP
Eth1/42

c1(FOX2025GEEX)     Eth1/43        175    S I s      N5K-C5596UP
Eth1/43

c1(FOX2025GEEX)     Eth1/44        175    S I s      N5K-C5596UP
Eth1/44

c1(FOX2025GEEX)     Eth1/45        175    S I s      N5K-C5596UP
Eth1/45

c1(FOX2025GEEX)     Eth1/46        175    S I s      N5K-C5596UP
Eth1/46

c1(FOX2025GEEX)     Eth1/47        176    S I s      N5K-C5596UP
Eth1/47

c1(FOX2025GEEX)     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 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
```

```
cluster1::*> 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    cs2                       0/2               N9K-
C92300YC
node1      /cdp
             e0a    c1                        0/1               N5K-
C5596UP
             e0b    cs2                       0/1               N9K-
C92300YC

4 entries were displayed.
```

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
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
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
--------- ----------- --------------- ---- ---- ----------- --------
------
e0a       Cluster     Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster     Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster     Cluster          up   9000  auto/10000 healthy
false

4 entries were displayed.


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.
```

```
cluster1::*> 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

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         124    H         FAS2750
e0a
node2               Eth1/2         124    H         FAS2750
e0a
cs2(FDO220329V5)    Eth1/65        179    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        179    R S I s   N9K-C92300YC
Eth1/66


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          124     H           FAS2750
e0b
node2                   Eth1/2          124     H           FAS2750
e0b
cs1(FDO220329KU)
                        Eth1/65         179     R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                        Eth1/66         179     R S I s     N9K-C92300YC
Eth1/66

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     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)


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       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
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
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
4 entries were displayed.



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.



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
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    H           FAS2980       e0a
node2              Eth1/2         145    H           FAS2980       e0a
cs2(FDO220329V5)   Eth1/65        176    R S I s     N9K-C92300YC  Eth1/65
cs2(FDO220329V5)   Eth1/66        176    R S I s     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    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC  Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC  Eth1/66
```

```
Total entries displayed: 4
```

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
Vserver      Interface     Auto-revert
------------ ------------- -------------
Cluster      node1_clus1   true
Cluster      node1_clus2   true
Cluster      node2_clus1   true
Cluster      node2_clus2   true

4 entries were displayed.
```

4. 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)
```

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
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)

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 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       Cluster      Cluster          up   9000  auto/10000  healthy
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
e0b       Cluster      Cluster          up   9000  auto/auto   -
false

4 entries were displayed.
```

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 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      e0a
false

4 entries were 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 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       Cluster     Cluster           up    9000  auto/10000  healthy
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
e0b       Cluster      Cluster          up    9000  auto/10000  healthy
false

4 entries were displayed.
```

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`

```
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       Cluster     Cluster          up   9000  auto/10000  healthy
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
e0b       Cluster      Cluster          up   9000 auto/10000  healthy
false

4 entries were displayed.


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.

cluster1::> 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    newcs2                    0/2               N9K-
```

```
C92300YC
node1      /cdp
            e0a    cs1                        0/1               N9K-
C92300YC
            e0b    newcs2                     0/1               N9K-
C92300YC

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    H           FAS2980       e0a
node2                Eth1/2         145    H           FAS2980       e0a
newcs2(FDO296348FU)  Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
newcs2(FDO296348FU)  Eth1/66        176    R S I s     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    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
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 commamds:

`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.

NVIDIA SN2100 Switches

NVIDIA SN2100 switch

From ONTAP 9.10.1P3, you can use NVIDIA SN2100 switches to combine storage and cluster functionality into a shared switch confguration.

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 install the NVIDIA SN2100 switch (X190006/X190106) in the NVIDIA dual/single switch cabinet with the standard brackets that are included with the switch.

SN2100 switches and rail kit details

The following table lists the part number and description for the MSN2100 switches and rail kits:

Part number	Description
X190006-PE	Cluster Switch, NVIDIA SN2100, 16PT 100G, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16PT 100G, PSIN
X190106-FE-PE	Switch, NVIDIA SN2100, 16PT 100G, PTSX, Front End
X190106-FE-PI	Switch, NVIDIA SN2100, 16PT 100G, PSIN, Front End
X-MTEF-KIT-D	Rail Kit, NVIDIA Dual switch side by side
X-MTEF-KIT-E	Rail Kit, NVIDIA Single switch short depth

See NVIDIA documentation for details on installing your SN2100 switch and rail kit.

Available documentation

The following table lists the documentation available for the NVIDIA SN2100 switches.

Title	Description
Setup and configure your NVIDIA SN2100 switches	Describes how to setup and configure your NVIDIA SN2100 switches, including installing Cumulus Linux and applicable RCFs.
Migrate from a Cisco cluster switch to a NVIDIA SN2100 cluster switch	Describes how to migrate from environments that use Cisco cluster switches to environments that use NVIDIA SN2100 cluster switches.
Migrate from a Cisco storage switch to a NVIDIA storage switch	Describes how to migrate from environments that use Cisco storage switches to environments that use NVIDIA SN2100 storage switches.

Title	Description
Migrate to a two-node switched cluster with NVIDIA SN2100 cluster switches	Describes how to migrate to a two-node switched environment using NVIDIA SN2100 cluster switches.
Replace a NVIDIA SN2100 cluster switch	Describes the procedure to replace a defective NVIDIA SN2100 switch in a cluster and download Cumulus Linux and reference configuration file.
Replace a NVIDIA SN2100 storage switch	Describes the procedure to replace a defective NVIDIA SN2100 storage switch and download Cumulus Linux and reference configuration file.

Setup and configure NVIDIA SN2100 switches

Setup and configure the NVIDIA SN2100 switches

The NVIDIA SN2100 switch is a 10/25/40/100 Gb Ethernet switch running Cumulus Linux. The SN2100 switch serves Cluster and Storage applications in ONTAP 9.10.1P3 over different switch-pairs.

Cumulus Linux (CL) OS can be installed either when the switch is running Cumulus Linux or ONIE.
For this release, Cumulus Linux version 4.4.2 is supported.

> ℹ The procedures here use Network Command Line Utility (NCLU) which is a command line interface that ensures Cumulus Linux is fully accessible to all. The net command is the wrapper utility you use to execute actions from a terminal.

> ℹ When using breakout cables for 10G and 25G, make sure that auto-negotiation is off and hard set the port speed on the switch. See Cabling and configuration considerations for further details.

Cabling and configuration considerations

Before configuring your NVIDIA SN2100 switch, review the following information:

1. Only optical connections are supported on SN2100 switches with X1151A NIC, X1146A NIC, or onboard 100GbE ports. For example:
   a. AFF A800 on ports e0a and e0b
   b. AFF A320 on ports e0g and e0h
2. When a QSA adapter is used to connect to the onboard Intel cluster ports on a platform, not all links come up.

   Example platforms are: FAS2750, AFF A300, and FAS8200 (all 10G) and AFF A250 (25G).

   To resolve this issue, do the following:

   a. For Intel 10G, manually set the swp1s0-3 link speed to 10000 and set auto-negotiation to off

b. For Chelsio 25G, manually set the swp2s0-3 link speed to 25000 and set auto-negotiation to off

> ⓘ Using 10G/25G QSA, use the non-breakout 40/100G ports. Do not insert the QSA adapter on ports that are configured for breakout.

3. Depending on the transceiver in the switchport, you might need to set the speed on the switchport to fixed speed. If using 10G and 25G breakout ports, make sure that auto-negotiation is off and hard set the port speed on the switch. For example:

```
cumulus@cumulus:mgmt:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces     2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000  <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp1s3
iface swp1s3
     alias 10G Intra-Cluster Node
-    link-autoneg off
+    link-autoneg on
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp2s0
iface swp2s0
     alias 25G Intra-Cluster Node
     link-autoneg off
     link-speed 25000 <---- port speed set
```

Install Cumulus Linux in Cumulus mode

Cumulus Linux (CL) OS can be installed either when the switch is running Cumulus Linux or ONIE.

Before you begin

The following assumptions are made:

- You have intermediate-level Linux knowledge.

- You are familiar with basic text editing, UNIX file permissions, and process monitoring. A variety of text editors are pre-installed, including `vi` and `nano`.
- You must have access to a Linux or UNIX shell. If you are running Windows, use a Linux environment as your command line tool for interacting with Cumulus Linux.

Each time Cumulus Linux is installed, the entire file system structure is erased and rebuilt.

The default password for the cumulus user account is **cumulus**. The first time you log into Cumulus Linux, you must change this default password. Be sure to update any automation scripts before installing a new image. Cumulus Linux provides command line options to change the default password automatically during the installation process.

The baud rate requirement must be set to 115200 on the serial console switch for NVIDIA SN2100 switch console access, as follows:

- 115200 baud
- 8 data bits
- 1 stop bit
- parity: none
- flow control: none

Steps

1. Log in to the switch. First time log in to the switch requires username/password of **cumulus**/**cumulus** with `sudo` privileges:

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: netapp1!
Retype new password: netapp1!
```

2. Check the Cumulus Linux version:

```
cumulus@cumulus:mgmt:~$ net show system
Hostname......... cumulus
Build............ Cumulus Linux 4.4.2
Uptime........... 0:08:20.860000
Model............ Mlnx X86
CPU.............. x86_64 Intel Atom C2558 2.40GHz
Memory........... 8GB
Disk............. 14.7GB
ASIC............. Mellanox Spectrum MT52132
Ports............ 16 x 100G-QSFP28
Part Number...... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Configure the hostname, IP address, subnet mask, and default gateway. The new hostname only becomes effective after restarting the console/SSH session.

   A Cumulus Linux switch provides at least one dedicated Ethernet management port called `eth0`. This interface is specifically for out-of-band management use. By default, the management interface uses DHCPv4 for addressing.

   Do not use an underscore (_), apostrophe ('), or non-ASCII characters in the hostname.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address 10.233.204.71
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

   This command modifies both the `/etc/hostname` and `/etc/hosts` files.

4. Confirm that the hostname, IP address, subnet mask, and default gateway have been updated:

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device memory
0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Configure the time zone using NTP interactive mode.
   a. On a terminal, run the following command:

   ```
   cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
   ```

   b. Follow the on-screen menu options to select the geographic area and region.
   c. To set the time zone for all services and daemons, reboot the switch.
   d. Verify that the date and time on the switch are correct and update if necessary.
6. Install Cumulus Linux 4.4.2:

   ```
   cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
   server>/<path>/cumulus-linux-4.4.2-mlx-amd64.bin
   ```

   The installer starts the download. Type **y** when prompted.

7. Reboot the NVIDIA SN2100 switch:

   ```
   cumulus@sw1:mgmt:~$ sudo reboot
   ```

8. The installation starts automatically, and the following GRUB screens appear. Do **not** make any selections:
   - Cumulus-Linux GNU/Linux
   - ONIE: Install OS
   - CUMULUS-INSTALL

- Cumulus-Linux GNU/Linux

9. Repeat steps 1 to 4 to log in.
10. Verify that the Cumulus Linux version is 4.4.2:

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.2u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.2
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.2"
```

11. Create a new user and add this user to the `sudo` group. This user only becomes effective after the console/SSH session is restarted:

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user `admin’ ...
Adding new user `admin’ (1001) with group `netedit' ...
Creating home directory `/home/admin’ ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1 (2021-
09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a
world-wide basis.
admin@sw1:mgmt:~$
```

Install Cumulus Linux in ONIE mode

Cumulus Linux (CL) OS can be installed either when the switch is running Cumulus Linux or ONIE.

Before you begin

You can install the Cumulus Linux using Open Network Install Environment (ONIE) that allows for automatic discovery of a network installer image. This facilitates the system model of securing switches with an operating system choice, such as Cumulus Linux. The easiest way to install Cumulus Linux with ONIE is with local HTTP discovery.

> If your host is IPv6-enabled, make sure it is running a web server. If your host is IPv4-enabled, make sure it is running DHCP in addition to a web server.

This procedure demonstrates how to upgrade Cumulus Linux after the admin has booted in ONIE.

Steps

1. Download the Cumulus Linux installation file to the root directory of the web server. Rename this file `onie-installer`.
2. Connect your host to the management Ethernet port of the switch using an Ethernet cable.
3. Power on the switch. The switch downloads the ONIE image installer and boots. After the installation completes, the Cumulus Linux login prompt appears in the terminal window.

   > Each time Cumulus Linux is installed, the entire file system structure is erased and rebuilt.

4. Reboot the SN2100 switch:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

5. Hit the **Esc** key at the GNU GRUB screen to interrupt the normal boot process, select **ONIE** and press Enter.
6. On the next screen displayed, select **ONIE: Install OS**.
7. The ONIE installer discovery process runs searching for the automatic installation. Press Enter to temporarily stop the process.
8. When the discovery process has stopped:

```
ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover...start-stop-daemon: warning: killing process 427:
No such process done.
```

9. If the DHCP service is running on your network, verify that the IP address, subnet mask, and the default gateway are correctly assigned:

```
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
       inet addr:10.233.204.71  Bcast:10.233.205.255  Mask:255.255.254.0
       inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
       TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
       Memory:dfc00000-dfc1ffff

ONIE:/ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface

default         10.233.204.1    0.0.0.0         UG    0      0      0
eth0
10.233.204.0    *               255.255.254.0   U     0      0      0
eth0
```

10. If the IP addressing scheme is manually defined, do the following:

```
ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1
```

11. Repeat step 9 to verify that the static information is correctly entered.
12. Install Cumulus Linux:

```
ONIE:/ # route

  Kernel IP routing table

  ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-linux-
4.4.2-mlx-amd64.bin

  Stopping: discover... done.
  Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-4.4.2-
mlx-amd64.bin ...
  Connecting to 10.60.132.97 (10.60.132.97:80)
  installer            100% |*|   552M  0:00:00 ETA
  ...
  ...
```

13. Once the installation has completed, log in to the switch:

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: netapp1!
Retype new password: netapp1!
```

14. Verify the Cumulus Linux version:

```
cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.2u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.2
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.2"
```

Install the RCF script

Before installing the RCF script, ensure that the following are available on the switch:

- Cumulus Linux 4.4.2 is installed.
- IP address, subnet mask, and default gateway defined via DHCP or manually configured.

> See Cabling and configuration considerations for caveats and further details.

Current RCF script versions

There are two RCF scripts available for Clustering and Storage applications. The procedure for each is the same.

- Clustering: **MSN2100-RCF-v1.8-Cluster**
- Storage: **MSN2100-RCF-v1.8-Storage**

> The following example procedure shows how to download and apply the RCF script for Cluster switches.

> Example command output uses switch management IP address 10.233.204.71, netmask 255.255.254.0 and default gateway 10.233.204.1.

Steps

1. Display the available interfaces on the SN2100 switch:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name   Spd  MTU   Mode         LLDP                 Summary
-----  -----  ---  ----- -----------  ------------------
--------------
...
...
ADMDN  swp1   N/A  9216  NotConfigured
ADMDN  swp2   N/A  9216  NotConfigured
ADMDN  swp3   N/A  9216  NotConfigured
ADMDN  swp4   N/A  9216  NotConfigured
ADMDN  swp5   N/A  9216  NotConfigured
ADMDN  swp6   N/A  9216  NotConfigured
ADMDN  swp7   N/A  9216  NotConfigure
ADMDN  swp8   N/A  9216  NotConfigured
ADMDN  swp9   N/A  9216  NotConfigured
ADMDN  swp10  N/A  9216  NotConfigured
ADMDN  swp11  N/A  9216  NotConfigured
ADMDN  swp12  N/A  9216  NotConfigured
ADMDN  swp13  N/A  9216  NotConfigured
ADMDN  swp14  N/A  9216  NotConfigured
ADMDN  swp15  N/A  9216  NotConfigured
ADMDN  swp16  N/A  9216  NotConfigured
```

2. Copy the RCF python script to the switch:

```
cumulus@cumulus:mgmt:~$ pwd
/home/cumulus
cumulus@cumulus:mgmt: /tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.8-
Cluster
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.8-Cluster                  100% 8607   111.2KB/s
00:00
```

3. Apply the RCF python script **MSN2100-RCF-v1.8-Cluster**:

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.8-Cluster
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

The RCF script completes the following steps:

a. Updates the banner MOTD
b. Disables the apt-get for OS updates
c. Defines breakout and non-breakout interfaces
d. Configures interfaces and SNMP
e. Disables CDP
f. Changes the LLDP configuration
g. Adds a RoCE configuration
h. Modifies the RoCE configuration for HA and Cluster RDMA
i. Reboots the switch

> For any RCF python script issues that cannot be corrected, contact NetApp Support for assistance.

4. Verify the configuration after the reboot:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name       Spd   MTU    Mode        LLDP                 Summary
-----  ---------  ----  -----  ----------  -----------------  --------
...
...
DN     swp1s0     N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp1s1     N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp1s2     N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp1s3     N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp2s0     N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp2s1     N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp2s2     N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp2s3     N/A   9216   Trunk/L2                        Master:
bridge(UP)
UP     swp3       100G  9216   Trunk/L2                        Master:
bridge(UP)
UP     swp4       100G  9216   Trunk/L2                        Master:
bridge(UP)
DN     swp5       N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp6       N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp7       N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp8       N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp9       N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp10      N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp11      N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp12      N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp13      N/A   9216   Trunk/L2                        Master:
bridge(UP)
DN     swp14      N/A   9216   Trunk/L2                        Master:
```

```
bridge(UP)
UP     swp15     N/A   9216   BondMember                   Master:
bond_15_16(UP)
UP     swp16     N/A   9216   BondMember                   Master:
bond_15_16(UP)
...
...

cumulus@cumulus:mgmt:~$ net show roce config
RoCE mode.......... lossless
Congestion Control:
  Enabled SPs.... 0 2 5
  Mode........... ECN
  Min Threshold.. 150 KB
  Max Threshold.. 1500 KB
PFC:
  Status......... enabled
  Enabled SPs.... 2 5
  Interfaces......... swp10-16,swp1s0-3,swp2s0-3,swp3-9

DSCP                      802.1p  switch-priority
-----------------------  ------  ---------------
0 1 2 3 4 5 6 7               0                0
8 9 10 11 12 13 14 15         1                1
16 17 18 19 20 21 22 23       2                2
24 25 26 27 28 29 30 31       3                3
32 33 34 35 36 37 38 39       4                4
40 41 42 43 44 45 46 47       5                5
48 49 50 51 52 53 54 55       6                6
56 57 58 59 60 61 62 63       7                7

switch-priority  TC  ETS
---------------  --  --------
0 1 3 4 6 7       0  DWRR 28%
2                 2  DWRR 28%
5                 5  DWRR 43%
```

5. Verify information for the transceiver in the interface:
`net show interface pluggables`

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
Interface  Identifier     Vendor Name  Vendor PN        Vendor SN
Vendor Rev
---------  -------------  -----------  ---------------  --------------
----------
swp3       0x11 (QSFP28)  Amphenol     112-00574        APF20379253516
B0
swp4       0x11 (QSFP28)  AVAGO        332-00440        AF1815GU05Z
A0
swp15      0x11 (QSFP28)  Amphenol     112-00573        APF21109348001
B0
swp16      0x11 (QSFP28)  Amphenol     112-00573        APF21109347895
B0
```

6. Verify that the nodes each have a connection to each switch:
   `net show lldp`

```
cumulus@cumulus:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost             RemotePort
---------  -----  ----------  ---------------------  -----------
swp3       100G   Trunk/L2    sw1                    e3a
swp4       100G   Trunk/L2    sw2                    e3b
swp15      100G   BondMember  sw13                   swp15
swp16      100G   BondMember  sw14                   swp16
```

7. 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: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

b. Verify the switch health from the cluster (this might not show switch sw2, since LIFs are not homed on e0d).

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address          Model
--------------------------- ------------------ ---------------- -----
sw1                         cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.2 running on Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                         cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.2 running on Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

Configure SNMPv3 for switch log collection

This release includes support for SNMPv3 for switch log collection for Switch Health Monitoring (SHM).

About this task

The following commands configure an SNMPv3 username on NVIDIA SN2100 switches:

- For **no authentication**:
  `net add snmp-server username` *`SNMPv3_USER`* `auth-none`

* For **MD5/SHA authentication**:
  `net add snmp-server username` *`SNMPv3_USER`* `[auth-md5|auth-sha]` *`AUTH-PASSWORD`*
* For **MD5/SHA authentication with AES/DES encryption**:
  `net add snmp-server username` *`SNMPv3_USER`* `[auth-md5|auth-sha]` *`AUTH-PASSWORD`* `[encrypt-aes|encrypt-des]` *`PRIV-PASSWORD`*

The following command configures an SNMPv3 username on the ONTAP side:
`cluster1::*> security login create -user-or-group-name` *`SNMPv3_USER`* `-application snmp -authentication-method usm -remote-switch-ipaddress` *`ADDRESS`*

The following command establishes the SNMPv3 username with SHM:
`cluster1::*> system switch ethernet modify -device` *`DEVICE`* `-snmp-version SNMPv3 -community-or-username` *`SNMPv3_USER`*

Steps

1. Setup the SNMPv3 user on the switch to use authentication and encryption:

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     4318
Version 1 and 2c Community String  Configured
Version 3 Usernames                Not Configured
---------------------------------  ----------------
cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5 netapp1!
encrypt-aes netapp1!
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf        2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf   2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
 # Auto-generated config file: do not edit. #
 agentaddress udp:@mgmt:161
 agentxperms 777 777 snmp snmp
 agentxsocket /var/agentx/master
 createuser _snmptrapusernameX
+createuser SNMPv3User MD5 netapp1! AES netapp1!
 ifmib_max_num_ifaces 500
 iquerysecname _snmptrapusernameX
 master agentx
 monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0
 pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
 pass_persist 1.2.840.10006.300.43 /usr/share/snmp/ieee8023_lag_pp.py
 pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
```

```
 pass_persist 1.3.6.1.2.1.31.1.1.1.18 /usr/share/snmp/snmpifAlias_pp.py
 pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
 pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
 pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
 pass_persist 1.3.6.1.4.1.40310.2 /usr/share/snmp/cl_drop_cntrs_pp.py
 pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
 pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
 pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
 pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
 pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshm1! default
 rouser _snmptrapusernameX
+rouser SNMPv3User priv
 sysobjectid 1.3.6.1.4.1.40310
 sysservices 72
-rocommunity cshm1! default


net add/del commands since the last "net commit"
================================================

User        Timestamp                   Command
----------  --------------------------
--------------------------------------------------------------------------
-----
SNMPv3User  2020-08-11 00:13:51.826987  net add snmp-server username
SNMPv3User auth-md5 netapp1! encrypt-aes netapp1!

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     24253
Version 1 and 2c Community String  Configured
Version 3 Usernames                Configured     <---- Configured here
---------------------------------  ----------------
cumulus@sw1:~$
```

2. Setup the SNMPv3 user on the ONTAP side:

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128) [none]:
aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configure SHM to monitor with the new SNMPv3 user:

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                   Device Name: sw1 (b8:59:9f:09:7c:22)
                                    IP Address: 10.231.80.212
                                  SNMP Version: SNMPv2c
                                 Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                  Model Number: MSN2100-CB2FC
                                Switch Network: cluster-network
                              Software Version: Cumulus Linux version
4.4.3 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Verify that the serial number to be queried with the newly created SNMPv3 user is the same as detailed in the previous step once the SHM polling period has completed.

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                   Device Name: sw1 (b8:59:9f:09:7c:22)
                                    IP Address: 10.231.80.212
                                  SNMP Version: SNMPv3
                                 Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: SNMPv3User
                                  Model Number: MSN2100-CB2FC
                                Switch Network: cluster-network
                              Software Version: Cumulus Linux version
4.4.3 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

Cable NS224 shelves as switch-attached storage

If you have a system in which the NS224 drive shelves need to be cabled as switch-attached storage (not direct-attached storage), use the information provided here.

- Cable NS224 drive shelves through storage switches:

  Information for cabling switch-attached NS224 drive shelves

- Install your storage switches:

  AFF and FAS Switch Documentation

- Confirm supported hardware, such as storage switches and cables, for your platform model:

  NetApp Hardware Universe

Migrate from a Cisco cluster switch to a NVIDIA SN2100 cluster switch

You can migrate nondisruptively Cisco cluster switches for an ONTAP cluster to NVIDIA SN2100 cluster switches. You must be aware of certain configuration information, port connections and cabling requirements when you are replacing some older Cisco cluster switches with NVIDIA SN2100 cluster switches.

The following Cisco cluster switches are supported:

- Nexus 9336C-FX2
- Nexus 92300YC
- Nexus 5596UP
- Nexus 3232C
- Nexus 3132Q-V

Before you begin

You can migrate nondisruptively older Cisco cluster switches for an ONTAP cluster to NVIDIA SN2100 cluster 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 NVIDIA SN2100 cluster switches must be configured and operating under the proper version of Cumulus Linux installed with the 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.
- See the Hardware Universe for full details of supported ports and their configurations.
- You have configured some of the ports on NVIDIA SN2100 switches to run at 40 GbE or 100 GbE.
- You have planned, migrated, and documented 40 GbE and 100 GbE connectivity from nodes to NVIDIA SN2100 cluster switches.

> In this procedure, Cisco Nexus 3232C cluster switches are used for example commands and outputs.

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 NVIDIA SN2100 cluster switches are *sw1* and *sw2*.
- 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.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The cluster ports used in this procedure are *e3a* and *e3b*.
- Breakout ports take the format: swp[port]s[breakout port 0-3]. For example, four breakout ports on swp1 are *swp1s0*, *swp1s1*, *swp1s2*, and *swp1s3*.

- Switch c2 is replaced by switch sw2 first and then switch c1 is replaced by switch sw1.
  - Cabling between the nodes and c2 are then disconnected from c2 and reconnected to sw2.
  - Cabling between the nodes and c1 are then disconnected from c1 and reconnected to sw1.

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. Change the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

   The advanced prompt (*>) appears.

3. Disable auto-revert on the cluster LIFs: `network interface modify -vserver Cluster -lif * -auto-revert false`

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

Warning: Disabling the auto-revert feature of the cluster logical
interface may effect the availability of your cluster network. Are you
sure you want to continue? {y|n}: y
```

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 port show -ipspace Cluster

Node: node1

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: node2

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
```

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
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
```

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 lldp`

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node1      /lldp
            e3a    c1 (6a:ad:4f:98:3b:3f)    Eth1/1            -
            e3b    c2 (6a:ad:4f:98:4c:a4)    Eth1/1            -
node2      /lldp
            e3a    c1 (6a:ad:4f:98:3b:3f)    Eth1/2            -
            e3b    c2 (6a:ad:4f:98:4c:a4)    Eth1/2            -
```

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

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         124   H           AFF-A400
e3a
node2                 Eth1/2         124   H           AFF-A400
e3a
c2                    Eth1/31        179   S I s       N3K-C3232C
Eth1/31
c2                    Eth1/32        175   S I s       N3K-C3232C
Eth1/32

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
node1                 Eth1/1        124    H           AFF-A400
e3b
node2                 Eth1/2        124    H           AFF-A400
e3b
c1                    Eth1/31       175    S I s       N3K-C3232C
Eth1/31
c1                    Eth1/32       175    S I s       N3K-C3232C
Eth1/32
```

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     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 169.254.19.183 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. On switch c2, shut down the ports connected to the cluster ports of the nodes.

```
(c2)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c2)(Config)# interface
(c2)(config-if-range)# shutdown <interface_list>
(c2)(config-if-range)# exit
(c2)(Config)# exit
(c2)#
```

9. Move the node cluster ports from the old switch c2 to the new switch sw2, using appropriate cabling supported by NVIDIA SN2100.
10. Display the network port attributes: `network port show -ipspace Cluster`

```
cluster1::*> network port show -ipspace Cluster

Node: node1

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: node2

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
```

11. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective:

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node1      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   Eth1/1            -
            e3b    sw2 (b8:ce:f6:19:1a:7e)   swp3              -
node2      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   Eth1/2            -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4              -
```

12. On switch sw2, verify that all node cluster ports are up: `net show interface`

```
cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP              Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b               Master:
bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b               Master:
bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)       Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)       Master:
cluster_isl(UP)
```

13. On switch c1, shut down the ports connected to the cluster ports of the nodes.

```
(c1)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c1)(Config)# interface
(c1)(config-if-range)# shutdown <interface_list>
(c1)(config-if-range)# exit
(c1)(Config)# exit
(c1)#
```

14. Move the node cluster ports from the old switch c1 to the new switch sw1, using appropriate cabling

supported by NVIDIA SN2100.

15. 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
--------- ---------- ---------------- ---- ----- ------------ --------
------
e3a       Cluster    Cluster          up   9000  auto/100000  healthy
false
e3b       Cluster    Cluster          up   9000  auto/100000  healthy
false

Node: node2

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
```

16. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective:

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface       Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3            -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3            -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4            -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4            -
```

17. On switches sw1 and sw2, verify that all node cluster ports are up: `net show interface`

```
cumulus@sw1:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP              Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3a               Master:
bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3a               Master:
bridge(UP)
UP     swp15        100G  9216   BondMember  sw2 (swp15)       Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw2 (swp16)       Master:
cluster_isl(UP)


cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP              Summary
-----  -----------  ----  -----  ----------  -----------------
-----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b               Master:
bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b               Master:
bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)       Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)       Master:
cluster_isl(UP)
```

18. Verify that both nodes each have one connection to each switch: `net show lldp`

    The following example shows the appropriate results for both switches:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3a
swp4       100G   Trunk/L2    node2               e3a
swp15      100G   BondMember  sw2                 swp15
swp16      100G   BondMember  sw2                 swp16

cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3b
swp4       100G   Trunk/L2    node2               e3b
swp15      100G   BondMember  sw1                 swp15
swp16      100G   BondMember  sw1                 swp16
```

19. Enable auto-revert on the cluster LIFs: `cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert true`
20. Verify that all cluster network LIFs are back on their home ports: `network interface show`

```
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         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
```

21. Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the 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:
sw1
sw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
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: sw2
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. Initiate the switch log collection feature: `system switch ethernet log collect -device *`

    Wait for 10 minutes and then check that the log collection was successful using the command: `system switch ethernet log show`

```
cluster1::*> system switch ethernet log show
Log Collection Enabled: true

Index  Switch                        Log Timestamp        Status
------ ----------------------------  -------------------  ---------
1      sw1 (b8:ce:f6:19:1b:42)       4/29/2022 03:05:25   complete
2      sw2 (b8:ce:f6:19:1b:96)       4/29/2022 03:07:42   complete
```

23. Change the privilege level back to admin: `set -privilege admin`
24. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=END`

Migrate from a Cisco storage switch to a NVIDIA SN2100 storage switch

You must be aware of certain configuration information, port connections and cabling requirements when you are replacing some older Cisco switches with NVIDIA SN2100 storage switches.

- The following storage switches are supported:
  - Cisco Nexus 9336C-FX2
  - Cisco Nexus 3232C
- See the Hardware Universe for full details of supported ports and their configurations.

Before you begin

You can migrate nondisruptively older Cisco storage switches for an ONTAP cluster to NVIDIA SN2100 storage switches.

- The existing cluster must be properly set up and functioning.
- All storage ports must be in the up state to ensure nondisruptive operations.
- The NVIDIA SN2100 storage switches must be configured and operating under the proper version of Cumulus Linux installed with the reference configuration file (RCF) applied.
- The existing storage 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.
- See the Hardware Universe for full details of supported ports and their configurations.
- You have configured some of the ports on NVIDIA SN2100 switches to run at 100 GbE.
- You have planned, migrated, and documented 100 GbE connectivity from nodes to NVIDIA SN2100 storage switches.

In this procedure, Cisco Nexus 9336C-FX2 storage switches are used for example commands and outputs.

About this task

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

- The existing Cisco Nexus 9336C-FX2 storage switches are *S1* and *S2*.
- The new NVIDIA SN2100 storage switches are *sw1* and *sw2*.
- 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.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The network ports used in this procedure are *e5a* and *e5b*.
- Breakout ports take the format: swp1s0-3. For example four breakout ports on swp1 are *swp1s0*, *swp1s1*, *swp1s2*, and *swp1s3*.
- Switch S2 is replaced by switch sw2 first and then switch S1 is replaced by switch sw1.
  - Cabling between the nodes and S2 are then disconnected from S2 and reconnected to sw2.
  - Cabling between the nodes and S1 are then disconnected from S1 and reconnected to sw1.

Steps

1. If AutoSupport is enabled, 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. Change the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

   The advanced prompt (*>) appears.

3. Determine the administrative or operational status for each storage interface:

   Each port should display enabled for `Status`.

   Display the network port attributes: `storage port show`

```
cluster1::*> storage port show
                                    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
cluster1::*>
```

4. The storage ports on each node are connected to existing storage switches in the following way (from the nodes' perspective) using the command: `network device-discovery show -protocol lldp`

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface       Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/1           -
            e5b    S2 (7c:ad:4f:98:8e:3c)    Eth1/1           -
node2      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/2           -
            e5b    S2 (7c:ad:4f:98:8e:3c)    Eth1/2           -
```

5. On switch S1 and S2, the storage ports and switches are connected in the following way (from the switches' perspective) using the command: `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     Holdtime    Capability
Port ID
node1                  Eth1/1         121         S
e0c
node2                  Eth1/2         121         S
e0c
SHFGD1947000186        Eth1/10        120         S
e0a
SHFGD1947000186        Eth1/11        120         S
e0a
SHFGB2017000269        Eth1/12        120         S
e0a
SHFGB2017000269        Eth1/13        120         S
e0a

S2# 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     Holdtime    Capability
Port ID
node1                  Eth1/1         121         S                  e5b
node2                  Eth1/2         121         S                  e5b
SHFGD1947000186        Eth1/10        120         S
 e0b
SHFGD1947000186        Eth1/11        120         S
 e0b
SHFGB2017000269        Eth1/12        120         S
 e0b
SHFGB2017000269        Eth1/13        120         S                  e0b
```

6. On switch sw2, shut down the ports connected to the storage ports and nodes of the disk shelves.

```
cumulus@sw2:~$ net add interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

7. Move the node storage ports of the controller and disk shelves from the old switch S2 to the new switch sw2, using appropriate cabling supported by NVIDIA SN2100.
8. On switch sw2, bring up the ports connected to the storage ports of the nodes and the disk shelves.

```
cumulus@sw2:~$ net del interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

9. The storage ports on each node are now connected to the switches in the following way, from the nodes' perspective:

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface      Platform
----------- ------ ------------------------- -------------
----------------
node1      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/1         -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp1           -

node2      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/2         -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp2           -
```

10. Verify the network port attributes: `storage port show`

```
cluster1::*> storage port show
                                     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
cluster1::*>
```

11. On switch sw2, verify that all node storage ports are up:

```
cumulus@sw2:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP                  Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e5b)             Master:
bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e5b)             Master:
bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)   Master:
bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)   Master:
bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)   Master:
bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)   Master:
bridge(UP))
...
...
```

12. On switch sw1, shut down the ports connected to the storage ports of the nodes and the disk shelves.

```
cumulus@sw1:~$ net add interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

13. Move the node storage ports of the controller and the disk shelves from the old switch S1 to the new switch sw1, using appropriate cabling supported by NVIDIA SN2100.
14. On switch sw1, bring up the ports connected to the storage ports of the nodes and the disk shelves.

```
cumulus@sw1:~$ net del interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

15. The storage ports on each node are now connected to the switches in the following way, from the nodes' perspective:

```
cluster1::*> network device-discovery show -protocol lldp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface       Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e0c    sw1 (b8:ce:f6:19:1b:96)   swp1            -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp1            -

node2      /lldp
            e0c    sw1  (b8:ce:f6:19:1b:96)  swp2            -
            e5b    sw2  (b8:ce:f6:19:1a:7e)  swp2            -
```

16. Verify the final configuration: `storage port show`

    Each port should display enabled for `State` and enabled for `Status`.

```
cluster1::*> storage port show
                                  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
cluster1::*>
```

17. On switch sw2, verify that all node storage ports are up:

```
cumulus@sw2:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP                  Summary
-----  ------  ----  -----  ----------  --------------------
-------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e5b)             Master:
bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e5b)             Master:
bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)   Master:
bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)   Master:
bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)   Master:
bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)   Master:
bridge(UP))
...
...
```

18. Verify that both nodes each have one connection to each switch: `net show lldp`

The following example shows the appropriate results for both switches:

```
cumulus@sw1:~$ net show lldp
LocalPort  Speed  Mode      RemoteHost             RemotePort
---------  -----  --------  ---------------------  -----------
...
swp1       100G   Trunk/L2  node1                  e0c
swp2       100G   Trunk/L2  node2                  e0c
swp3       100G   Trunk/L2  SHFFG1826000112        e0a
swp4       100G   Trunk/L2  SHFFG1826000112        e0a
swp5       100G   Trunk/L2  SHFFG1826000102        e0a
swp6       100G   Trunk/L2  SHFFG1826000102        e0a

cumulus@sw2:~$ net show lldp
LocalPort  Speed  Mode      RemoteHost             RemotePort
---------  -----  --------  ---------------------  -----------
...
swp1       100G   Trunk/L2  node1                  e5b
swp2       100G   Trunk/L2  node2                  e5b
swp3       100G   Trunk/L2  SHFFG1826000112        e0b
swp4       100G   Trunk/L2  SHFFG1826000112        e0b
swp5       100G   Trunk/L2  SHFFG1826000102        e0b
swp6       100G   Trunk/L2  SHFFG1826000102        e0b
```

19. Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the 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:
sw1
sw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
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: sw2
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.

20. Initiate the switch log collection feature: `system switch ethernet log collect -device *`

    Wait for 10 minutes and then check that the log collection was successful using the command: `system switch ethernet log show`

```
cluster1::*> system switch ethernet log show
Log Collection Enabled: true

Index  Switch                        Log Timestamp        Status
------ ----------------------------- -------------------  ---------
1      sw1 (b8:ce:f6:19:1b:42)      4/29/2022 03:05:25   complete
2      sw2 (b8:ce:f6:19:1b:96)      4/29/2022 03:07:42   complete
```

21. Change the privilege level back to admin: `set -privilege admin`
22. 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 NVIDIA SN2100 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 NVIDIA SN2100 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 10GBASE-T RJ45 ports for the cluster-network ports.

Two-node switchless configuration

- The two-node switchless configuration must be properly set up and functioning.
- The nodes must be running ONTAP 9.10.1P3 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.

NVIDIA SN2100 cluster switch configuration

- Both switches must have management network connectivity.
- There must be console access to the cluster switches.
- NVIDIA SN2100 node-to-node switch and switch-to-switch connections must use Twinax or fiber cables.

  > See Cabling and configuration considerations for caveats and further details.

  The Hardware Universe - Switches contains more information about cabling.

- Inter-Switch Link (ISL) cables must be connected to ports swp15 and swp16 on both NVIDIA SN2100 switches.
- Initial customization of both the SN2100 switches must be completed. So that the:
  - SN2100 switches are running the latest version of Cumulus Linux
  - 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 SN2100 switches are *sw1* and *sw2*.
- 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*.
- Breakout ports take the format: swp[port]s[breakout port 0-3]. For example, four breakout ports on swp1 are *swp1s0*, *swp1s1*, *swp1s2*, and *swp1s3*.

  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.

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 sw1 and sw2.

   You must not disable the ISL ports.

   The following commands disable the node-facing ports on switches sw1 and sw2:

   ```
   cumulus@sw1:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit

   cumulus@sw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link down
   cumulus@sw2:~$ net pending
   cumulus@sw2:~$ net commit
   ```

4. Verify that the ISL and the physical ports on the ISL between the two SN2100 switches sw1 and sw2 are up on ports swp15 and swp16: `net show interface`

   The following example shows that the ISL ports are up on switch sw1:

```
cumulus@sw1:~$ net show interface

State  Name       Spd   MTU    Mode        LLDP         Summary
-----  ---------  ----  -----  ----------  -----------
----------------------
...
...
UP     swp15      100G  9216   BondMember  sw2 (swp15)  Master:
cluster_isl(UP)
UP     swp16      100G  9216   BondMember  sw2 (swp16)  Master:
cluster_isl(UP)
```

The following example shows that the ISL ports are up on switch sw2:

```
cumulus@sw2:~$ net show interface

State  Name       Spd   MTU    Mode        LLDP         Summary
-----  ---------  ----  -----  ----------  -----------
----------------------
...
...
UP     swp15      100G  9216   BondMember  sw1 (swp15)  Master:
cluster_isl(UP)
UP     swp16      100G  9216   BondMember  sw1 (swp16)  Master:
cluster_isl(UP)
```

5. Verify that all cluster ports are up: `network port show`

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

```
cluster1::*> network port show

Node: node1


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: node2


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
```

6. Verify that all cluster LIFs are up and operational: `network interface show`

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

```
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         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
```

7. Disable auto-revert on the cluster LIFs: `network interface modify -vserver Cluster -lif * -auto-revert false`

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

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   false
          node1_clus2   false
          node2_clus1   false
          node2_clus2   false
```

8. Disconnect the cable from cluster port e3a on node1, and then connect e3a to port 3 on cluster switch sw1, using the appropriate cabling supported by the SN2100 switches.

   The Hardware Universe - Switches contains more information about cabling.

9. Disconnect the cable from cluster port e3a on node2, and then connect e3a to port 4 on cluster switch sw1, using the appropriate cabling supported by the SN2100 switches.
10. On switch sw1, enable all node-facing ports.

    The following command enables all node-facing ports on switch sw1:

```
cumulus@sw1:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

11. On switch sw1, verify that all ports are up: `net show interface all`

```
cumulus@sw1:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP             Summary
-----  --------- ----  -----  ---------- ---------------- --------
...
DN     swp1s0    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s1    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s2    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s3    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s0    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s1    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s2    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s3    25G   9216   Trunk/L2                    Master:
br_default(UP)
UP     swp3      100G  9216   Trunk/L2    node1 (e3a)     Master:
br_default(UP)
UP     swp4      100G  9216   Trunk/L2    node2 (e3a)     Master:
br_default(UP)
...
...
UP     swp15     100G  9216   BondMember  swp15           Master:
cluster_isl(UP)
UP     swp16     100G  9216   BondMember  swp16           Master:
cluster_isl(UP)
...
```

12. 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
--------- ------------ ---------------- ---- ---- ------------ --------
------
e3a       Cluster      Cluster          up   9000  auto/100000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/100000 healthy
false

Node: node2

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
```

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:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
```

14. Disconnect the cable from cluster port e3b on node1, and then connect e3b to port 3 on cluster switch sw2, using the appropriate cabling supported by the SN2100 switches.
15. Disconnect the cable from cluster port e3b on node2, and then connect e3b to port 4 on cluster switch sw2,

using the appropriate cabling supported by the SN2100 switches.

16. On switch sw2, enable all node-facing ports.

    The following commands enable the node-facing ports on switch sw2:

```
cumulus@sw2:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

17. On switch sw2, verify that all ports are up: `net show interface all`

```
cumulus@sw2:~$ net show interface all

State  Name      Spd  MTU    Mode       LLDP            Summary
-----  --------- ---- -----  ---------- --------------- --------
...
DN     swp1s0    10G  9216   Trunk/L2                   Master:
br_default(UP)
DN     swp1s1    10G  9216   Trunk/L2                   Master:
br_default(UP)
DN     swp1s2    10G  9216   Trunk/L2                   Master:
br_default(UP)
DN     swp1s3    10G  9216   Trunk/L2                   Master:
br_default(UP)
DN     swp2s0    25G  9216   Trunk/L2                   Master:
br_default(UP)
DN     swp2s1    25G  9216   Trunk/L2                   Master:
br_default(UP)
DN     swp2s2    25G  9216   Trunk/L2                   Master:
br_default(UP)
DN     swp2s3    25G  9216   Trunk/L2                   Master:
br_default(UP)
UP     swp3      100G 9216   Trunk/L2    node1 (e3b)    Master:
br_default(UP)
UP     swp4      100G 9216   Trunk/L2    node2 (e3b)    Master:
br_default(UP)
...
...
UP     swp15     100G 9216   BondMember  swp15          Master:
cluster_isl(UP)
UP     swp16     100G 9216   BondMember  swp16          Master:
cluster_isl(UP)
...
```

18. On both switches sw1 and sw2, verify that both nodes each have one connection to each switch: `net show lldp`

    The following example shows the appropriate results for both switches sw1 and sw2:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3a
swp4       100G   Trunk/L2    node2              e3a
swp15      100G   BondMember  sw2                swp15
swp16      100G   BondMember  sw2                swp16

cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3b
swp4       100G   Trunk/L2    node2              e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

19. Display information about the discovered network devices in your cluster: `net device-discovery show -protocol lldp`

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface      Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3           -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4           -
```

20. 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
--------- ------------ ---------------- ---- ---- ----------- --------
------
e3a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e3a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/10000 healthy
false
```

21. Enable auto-revert on all cluster LIFs: `net interface modify -vserver Cluster -lif * -auto -revert true`

```
cluster1::*> net interface modify -vserver Cluster -lif * -auto-revert
true

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true
```

22. Verify that all interfaces display true for `Is Home`: `net interface show -vserver Cluster`

> ⓘ This might take a minute to complete.

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

```
cluster1::*> net 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      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
```

23. Verify that the settings are disabled: `network options switchless-cluster show`

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

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

24. 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                true    true          false
node2                true    true          false
```

25. Ensure that the cluster network has full connectivity: `cluster ping-cluster -node node-name`

```
cluster1::*> cluster ping-cluster -node node1
Host is node1
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)
```

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` 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:
sw1
sw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
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: sw2
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.

27. Initiate the switch log collection feature: `system switch ethernet log collect -device *`

    Wait for 10 minutes and then check that the log collection was successful using the command: `system switch ethernet log show`

```
cluster1::*> system switch ethernet log show
Log Collection Enabled: true

Index  Switch                        Log Timestamp        Status
------ ---------------------------- -------------------  ---------
1      sw1 (b8:ce:f6:19:1b:42)      4/29/2022 03:05:25   complete
2      sw2 (b8:ce:f6:19:1b:96)      4/29/2022 03:07:42   complete
```

28. Change the privilege level back to admin: `set -privilege admin`
29. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=END`

Replace NVIDIA SN2100 switches

Replace a NVIDIA SN2100 cluster switch

Replacing a defective NVIDIA SN2100 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.
- NVIDIA SN2100 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 swp1 through swp14.
  - All Inter-Switch Link (ISL) ports must be disabled on ports swp15 and swp16.
  - The desired reference configuration file (RCF) and Cumulus operating system image switch must be loaded onto the switch.
  - Initial customization of the switch must be complete, as detailed in:

    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.

About this task

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

- The names of the existing NVIDIA SN2100 switches are *sw1* and *sw2*.
- The name of the new NVIDIA SN2100 switch is *nsw2*.
- 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::*>`
- Breakout ports take the format: swp[port]s[breakout port 0-3]. For example, four breakout ports on swp1 are *swp1s0*, *swp1s1*, *swp1s2*, and *swp1s3*.

> 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
--------- ------------ ---------------- ---- ---- ------------ --------
------
e3a       Cluster      Cluster          up   9000  auto/100000 healthy
false
e3b       Cluster      Cluster          up   9000  auto/100000 healthy
false

Node: node2

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
```

```
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         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


cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3          -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3          -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4          -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4          -
```

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    sw2                e3a
swp4       100G   Trunk/L2    sw2                e3a
swp15      100G   BondMember  sw2                swp15
swp16      100G   BondMember  sw2                swp16


cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    sw1                e3b
swp4       100G   Trunk/L2    sw1                e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

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. Change the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

   The advanced prompt (*>) appears.

3. Install the appropriate RCF and image on the switch, nsw2, and make any necessary site preparations.

   If necessary, verify, download, and install the appropriate versions of the RCF and Cumulus 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 Cumulus software, continue to step 3. See Setup and configure the NVIDIA SN2100 switches for further details.

   a. You can download the applicable Cumulus software for your cluster switches from the *NVIDIA Support* site. Follow the steps on the Download page to download the Cumulus Linux for the version of ONTAP software you are installing.

   b. The appropriate RCF is available from the *NVIDIA Cluster and Storage Switches* page. Follow the steps on the Download page to download the correct RCF for the version of ONTAP software you are installing.

4. On the new switch nsw2, log in as admin and shut down all of the ports that will be connected to the node cluster interfaces (ports swp1 to swp14).

   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.

```
cumulus@nsw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

5. Disable auto-revert on the cluster LIFs: `network interface modify -vserver Cluster -lif * -auto-revert false`

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

Warning: Disabling the auto-revert feature of the cluster logical
interface may effect the availability of your cluster network. Are you
sure you want to continue? {y|n}: y
```

6. Shut down the ISL ports swp15 and swp16 on the SN2100 switch sw1:

```
cumulus@sw1:~$ net add interface swp15-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

7. Remove all the cables from the SN2100 sw1 switch, and then connect them to the same ports on the SN2100 nsw2 switch.
8. Bring up the ISL ports swp15 and swp16 between the sw1 and nsw2 switches.

   The following commands enable ISL ports swp15 and swp16 on switch sw1:

```
cumulus@sw1:~$ net del interface swp15-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

   The following example shows that the ISL ports are up on switch sw1:

```
cumulus@sw1:~$ net show interface

State  Name          Spd   MTU    Mode        LLDP            Summary
-----  -----------   ----  -----  ----------  --------------
----------------------
...
...
UP     swp15         100G  9216   BondMember  nsw2 (swp15)    Master:
cluster_isl(UP)
UP     swp16         100G  9216   BondMember  nsw2 (swp16)    Master:
cluster_isl(UP)
```

The following example shows that the ISL ports are up on switch nsw2:

```
cumulus@nsw2:~$ net show interface

State  Name          Spd   MTU    Mode        LLDP            Summary
-----  -----------   ----  -----  ----------  -------------
-----------------------
...
...
UP     swp15         100G  9216   BondMember  sw1 (swp15)     Master:
cluster_isl(UP)
UP     swp16         100G  9216   BondMember  sw1 (swp16)     Master:
cluster_isl(UP)
```

9. Verify that port `e3b` is up on all nodes: `network port show -ipspace Cluster`

   The output should be similar to the following:

```
cluster1::*> network port show -ipspace Cluster

Node: node1

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: node2

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
```

10. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective:

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp3          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp3          -
node2      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp4          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp4          -
```

11. Verify that all node cluster ports are up: `net show interface`

```
cumulus@nsw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP              Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2                      Master:
bridge(UP)
UP     swp4         100G  9216   Trunk/L2                      Master:
bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)       Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)       Master:
cluster_isl(UP)
```

12. Verify that both nodes each have one connection to each switch: `net show lldp`

The following example shows the appropriate results for both switches:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3a
swp4       100G   Trunk/L2    node2              e3a
swp15      100G   BondMember  nsw2               swp15
swp16      100G   BondMember  nsw2               swp16


cumulus@nsw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1                e3b
swp4       100G   Trunk/L2    node2                e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

13. Enable auto-revert on the cluster LIFs: `cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert true`
14. On switch nsw2, bring up the ports connected to the network ports of the nodes.

```
cumulus@nsw2:~$ net del interface swp1-14 link down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

15. 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         true    true
node2         true    true
```

16. Verify that all physical cluster ports are up: `network port show ipspace Cluster`

```
cluster1::*> network port show -ipspace Cluster

Node node1
Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper  Status
Status
--------- ----------- ----------------- ----- ----- ----------- --------
------
e3a       Cluster     Cluster           up    9000  auto/10000  healthy
false
e3b       Cluster     Cluster           up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link  MTU   Admin/Oper  Status
Status
--------- ------------ ---------------- ----- ----- ----------- --------
------
e3a       Cluster      Cluster          up    9000  auto/10000  healthy
false
e3b       Cluster      Cluster          up    9000  auto/10000  healthy
false
```

17. Verify that the cluster network is healthy:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost      RemotePort
---------  -----  ----------  --------------  -----------
swp3       100G   Trunk/L2    node1           e3a
swp4       100G   Trunk/L2    node2           e3a
swp15      100G   BondMember  nsw2            swp15
swp16      100G   BondMember  nsw2            swp16
```

18. 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`

    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:
sw1
nsw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
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: nsw2
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.

19. Initiate the switch log collection feature: `system switch ethernet log collect -device *`

    Wait for 10 minutes and then check that the log collection was successful using the command: `system switch ethernet log show`

```
cluster1::*> system switch ethernet log show
Log Collection Enabled: true

Index  Switch                       Log Timestamp        Status
------ ---------------------------- -------------------  ---------
1      sw1  (b8:ce:f6:19:1b:42)      4/29/2022 03:05:25   complete
2      nsw2  (b8:ce:f6:19:1b:96)     4/29/2022 03:07:42   complete
```

20. Change the privilege level back to admin: `set -privilege admin`
21. 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 NVIDIA SN2100 storage switch

You must be aware of certain configuration information, port connections and cabling requirements when you replace NVIDIA SN2100 storage switches.

Before you begin

You must verify that the following conditions exist before installing the Cumulus software and RCFs on a NVIDIA SN2100 storage switch:

- Your system can support NVIDIA SN2100 storage switches.
- You must have downloaded the applicable RCFs.
- The Hardware Universe provides full details of supported ports and their configurations.

About this task

The existing network configuration must have the following characteristics:

- Ensure that all troubleshooting steps have been completed to confirm that your switch needs replacing.
- 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 NVIDIA SN2100 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 Cumulus operating system image must be loaded onto the switch.
- Initial customization of the switch must be complete.

Procedure summary

This procedure replaces the second NVIDIA SN2100 storage switch sw2 with the new NVIDIA SN2100 switch nsw2. The two nodes are node1 and node2.

Steps to complete:

- Confirm the switch to be replaced is sw2.
- Disconnect the cables from switch sw2.
- Reconnect the cables to switch nsw2.
- Verify all device configurations on switch nsw2.

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.

2. Change the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

3. 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`

```
cluster1::*> 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
cluster1::*>
```

4. Verify that storage switch sw1 is available:
   `network device-discovery show`

```
cluster1::*> network device-discovery show protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)   Interface   Platform
--------    ----   -----------------------    ---------   ---------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1b:42)    swp3        -
node2/lldp
            e3a    sw1 (b8:ce:f6:19:1b:42)    swp4        -
cluster1::*>
```

5. Run the `net show interface` command on the working switch to confirm that you can see both nodes and all shelves:
`net show interface`

```
cumulus@sw1:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP                    Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e3a)             Master:
bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e3a)             Master:
bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)   Master:
bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)   Master:
bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)   Master:
bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)   Master:
bridge(UP))
...
...
```

6. Verify the shelf ports in the storage system:
`storage shelf port show -fields remote-device, remote-port`

```
cluster1::*> storage shelf port show -fields remote-device, remote-port
shelf   id  remote-port   remote-device
-----   --  -----------   -------------
3.20    0   swp3          sw1
3.20    1   -             -
3.20    2   swp4          sw1
3.20    3   -             -
3.30    0   swp5          sw1
3.20    1   -             -
3.30    2   swp6          sw1
3.20    3   -             -
cluster1::*>
```

7. Remove all cables attached to storage switch sw2.
8. Reconnect all cables to the replacement switch nsw2.
9. Recheck the health status of the storage node ports:
   `storage port show -port-type ENET`

```
cluster1::*> 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
cluster1::*>
```

10. Verify that both switches are available:
    `net device-discovery show`

```
cluster1::*> network device-discovery show protocol lldp
Node/      Local Discovered
Protocol   Port  Device (LLDP: ChassisID)  Interface   Platform
--------   ----  -----------------------   ---------   ---------
node1/lldp
           e3a  sw1 (b8:ce:f6:19:1b:96)    swp1        -
           e7b  nsw2 (b8:ce:f6:19:1a:7e)   swp1        -
node2/lldp
           e3a  sw1 (b8:ce:f6:19:1b:96)    swp2        -
           e7b  nsw2 (b8:ce:f6:19:1a:7e)   swp2        -
cluster1::*>
```

11. Verify the shelf ports in the storage system:
`storage shelf port show -fields remote-device, remote-port`

```
cluster1::*> storage shelf port show -fields remote-device, remote-port
shelf   id    remote-port     remote-device
-----   --    -----------     -------------
3.20    0     swp3            sw1
3.20    1     swp3            nsw2
3.20    2     swp4            sw1
3.20    3     swp4            nsw2
3.30    0     swp5            sw1
3.20    1     swp5            nsw2
3.30    2     swp6            sw1
3.20    3     swp6            nsw2
cluster1::*>
```

12. Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the 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:
sw1
nsw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
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: nsw2
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.

13. Initiate the switch log collection feature: `system switch ethernet log collect -device *`

    Wait for 10 minutes and then check that the log collection was successful using the command: `system switch ethernet log show`

```
cluster1::*> system switch ethernet log show
Log Collection Enabled: true

Index  Switch                       Log Timestamp        Status
------ ---------------------------- -------------------  ---------
1      sw1 (b8:ce:f6:19:1b:42)      4/29/2022 03:05:25   complete
2      nsw2 (b8:ce:f6:19:1b:96)     4/29/2022 03:07:42   complete
```

14. Change the privilege level back to admin: `set -privilege admin`
15. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=END`

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

Other switch procedures

Transition to a two-node switchless cluster

Overview

If you have an existing two-node cluster that uses cluster interconnect switches and is running ONTAP 9.3 or later, you can replace the switches with direct, back-to-back connections between the nodes.

About this task

You cannot use the switchless cluster interconnect feature with more than two nodes.

Transitioning to a two-node switchless cluster configuration is a nondisruptive operation. Most systems have two dedicated cluster interconnect ports on each node, but you can also use this procedure for systems with a larger number of dedicated cluster interconnect ports on each node, such as four, six or eight.

This procedure describes transitioning a cluster with a switched cluster network to one where two nodes are directly connected for ONTAP 9.3 and later.

Replace the switches with direct connections

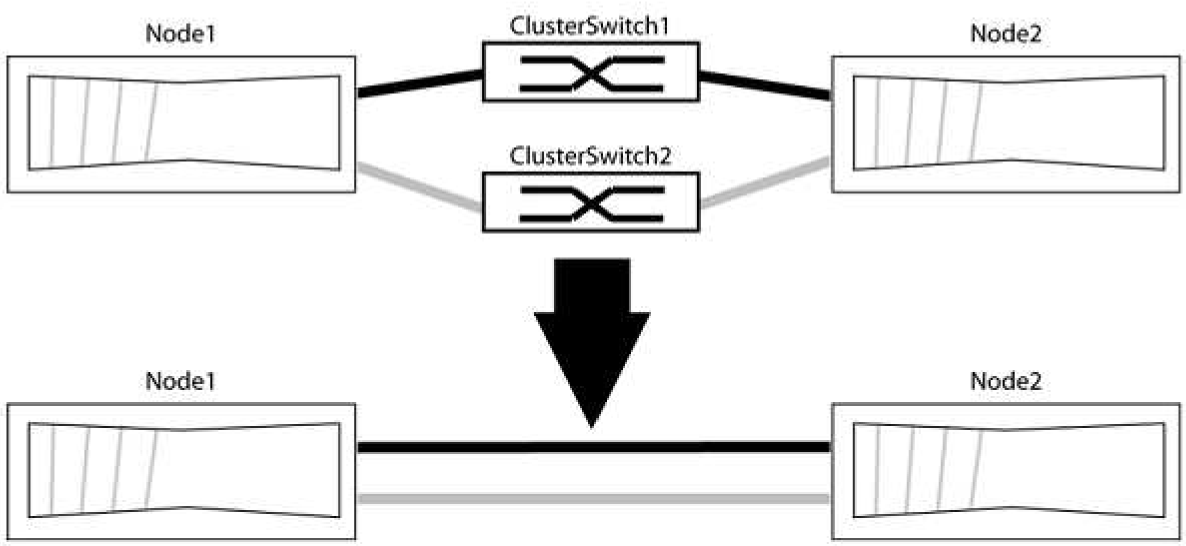
If you have a two-node cluster that uses cluster interconnect switches, replace the switches with direct, back-to-back connections between the nodes. This is a nondisruptive operation.

Before you begin

- The cluster must be healthy and consist of two nodes connected by cluster switches, and the nodes must be running the same ONTAP release.
- Each node must have the required number of dedicated cluster ports that provide redundant cluster interconnect connections to support your system configuration, for example, two redundant ports for a system with two dedicated cluster interconnect ports on each node.

About this task

The following procedure removes the cluster switches in a two-node cluster and replaces each connection to the switch with a direct connection to the partner node.



The examples in the following procedure show nodes that are using "e0a" and "e0b" as cluster ports. Your nodes might be using different cluster ports as they vary by system.

Steps

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

   `set -privilege advanced`

   The advanced prompt `*>` appears.

2. ONTAP 9.3 and later supports automatic detection of switchless clusters, which is enabled by default.

   You can verify that detection of switchless clusters is enabled by running the advanced privilege command:

   `network options detect-switchless-cluster show`

   The following example output shows if the option is enabled.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   If "Enable Switchless Cluster Detection” is `false`, contact support.

3. 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=<number_of_hours>h`

   where `h` is the duration of the maintenance window in hours. The message notifies technical support of this maintenance task so that they can suppress automatic case creation during the maintenance window.

   In the following example, the command suppresses automatic case creation for two hours:

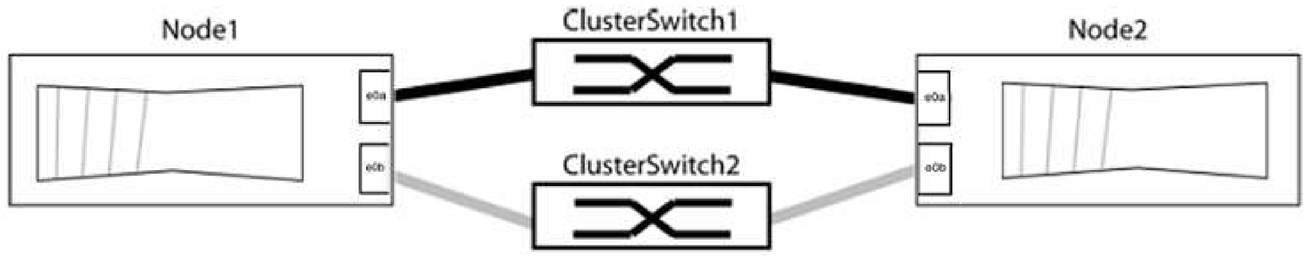
   ```
   cluster::*> system node autosupport invoke -node * -type all -message
   MAINT=2h
   ```

4. Organize the cluster ports on each switch into groups so that the cluster ports in group1 go to cluster switch1 and the cluster ports in group2 go to cluster switch2. These groups are required later in the procedure.

5. Identify the cluster ports and verify link status and health:

   `network port show -ipspace Cluster`

   In the following example for nodes with cluster ports "e0a" and "e0b", one group is identified as “node1:e0a” and “node2:e0a” and the other group as “node1:e0b” and “node2:e0b”. Your nodes might be using different cluster ports because they vary by system.



Verify that the ports have a value of `up` for the “Link” column and a value of `healthy` for the “Health Status” column, as shown in the following example:

```
cluster::> 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   Cluster   Cluster          up    9000  auto/10000  healthy 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
e0b   Cluster   Cluster          up    9000  auto/10000  healthy false
4 entries were displayed.
```

6. Confirm that all the cluster LIFs are on their home ports.

   Verify that the “is-home” column is `true` for each of the cluster LIFs:

   `network interface show -vserver Cluster -fields is-home`

   The system displays output similar to the following example:

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

If there are cluster LIFs that are not on their home ports, revert those LIFs to their home ports:

`network interface revert -vserver Cluster -lif *`

7. Disable auto-revert for the cluster LIFs:

   `network interface modify -vserver Cluster -lif * -auto-revert false`

8. Verify that all ports listed in the previous step are connected to a network switch:

   `network device-discovery show -port` *`cluster_port`*

   The “Discovered Device” column should be the name of the cluster switch that the port is connected to. The following example shows that cluster ports "e0a" and "e0b" are correctly connected to cluster switches "cs1" and "cs2".

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

9. Verify the cluster connectivity:

   `cluster ping-cluster -node local`

10. Verify that the cluster is healthy:

    `cluster ring show`

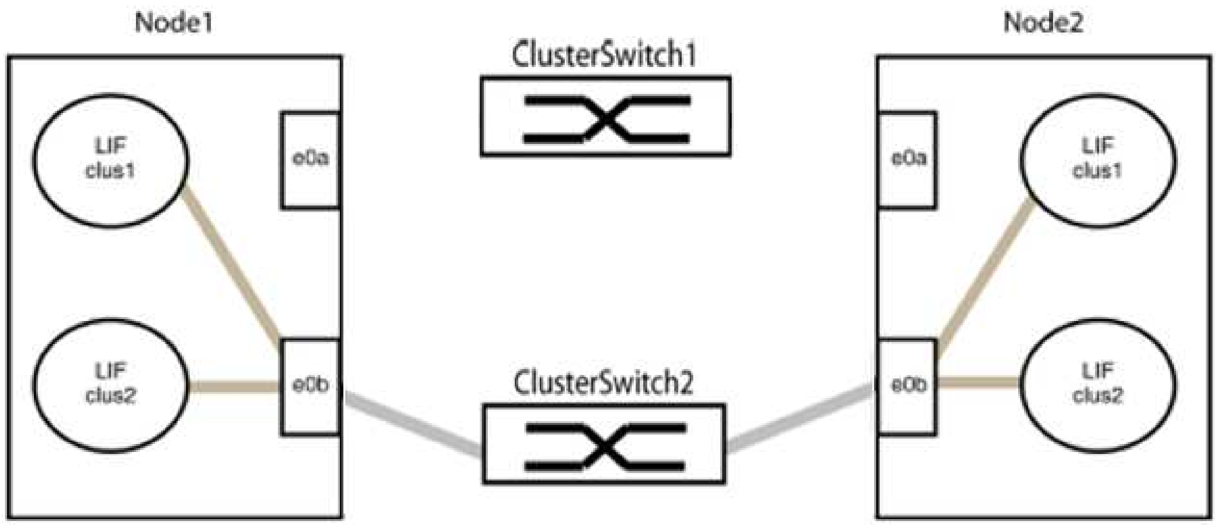
All units must be either master or secondary.

11. Set up the switchless configuration for the ports in group 1.

> To avoid potential networking issues, you must disconnect the ports from group1 and reconnect them back-to-back as quickly as possible, for example, **in less than 20 seconds**.

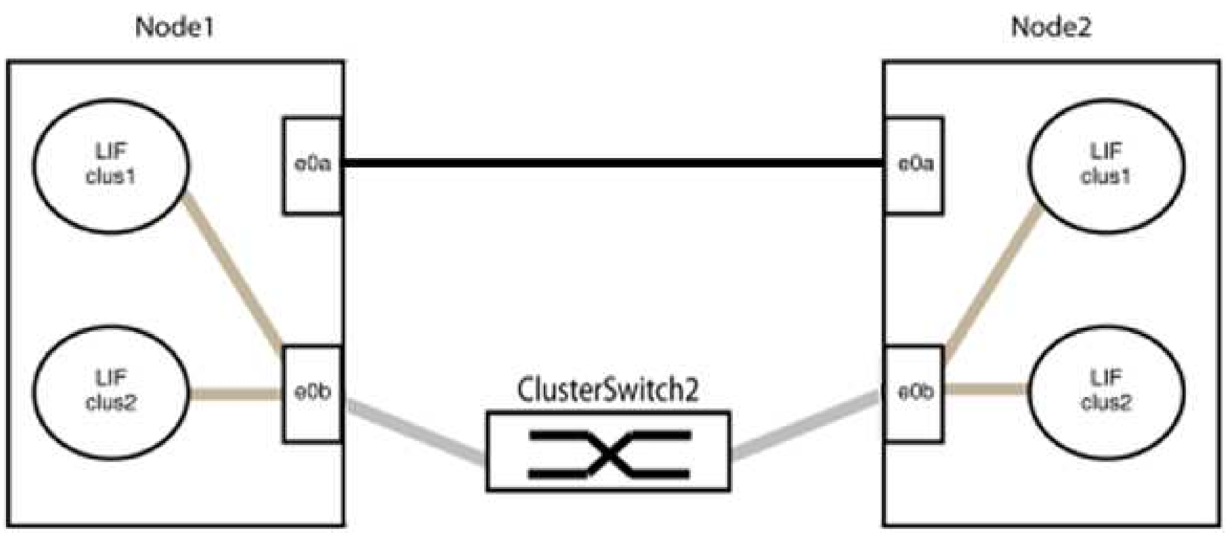
   a. Disconnect all the cables from the ports in group1 at the same time.

      In the following example, the cables are disconnected from port "e0a" on each node, and cluster traffic continues through the switch and port "e0b" on each node:



   b. Cable the ports in group1 back-to-back.

      In the following example, "e0a" on node1 is connected to "e0a" on node2:



12. The switchless cluster network option transitions from `false` to `true`. This might take up to 45 seconds. Confirm that the switchless option is set to `true`:

```
network options switchless-cluster show
```

The following example shows that the switchless cluster is enabled:

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

13. Verify that the cluster network is not disrupted:

```
cluster ping-cluster -node local
```

14. Set up the switchless configuration for the ports in group 2.

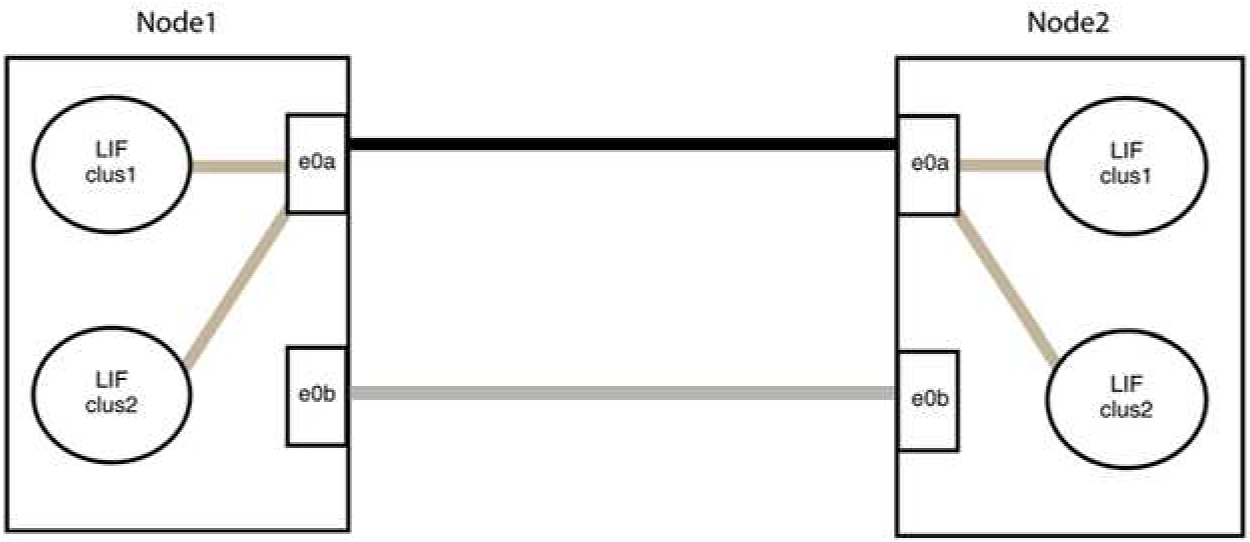
> To avoid potential networking issues, you must disconnect the ports from group2 and reconnect them back-to-back as quickly as possible, for example, **in less than 20 seconds**.

a. Disconnect all the cables from the ports in group2 at the same time.

In the following example, the cables are disconnected from port "e0b" on each node, and cluster traffic continues through the direct connection between the "e0a" ports:

b. Cable the ports in group2 back-to-back.

In the following example, "e0a" on node1 is connected to "e0a" on node2 and "e0b" on node1 is connected to "e0b" on node2:



15. Verify that the ports on both nodes are correctly connected:

    `network device-discovery show -port` *`cluster_port`*

    The following example shows that cluster ports "e0a" and "e0b" are correctly connected to the corresponding port on the cluster partner:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

16. Reenable auto-revert for the cluster LIFs:

    `network interface modify -vserver Cluster -lif * -auto-revert true`

17. Verify that all LIFs are home. This might take a few seconds:

`network interface show -vserver Cluster -lif lif_name`

The LIFs have been reverted if the “Is Home” column is `true`, as shown for `node1_clus2` and `node2_clus2` in the following example:

```
cluster::> network interface show -vserver Cluster -fields curr-port,is-
home
vserver  lif           curr-port is-home
-------- ------------- --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

If any cluster LIFS have not returned to their home ports, revert them manually:

`network interface revert -vserver Cluster -lif lif_name`

18. Check the cluster status of the nodes from the system console of either node:

    `cluster show`

    The following example shows epsilon on both nodes to be `false`:

```
Node  Health  Eligibility Epsilon
----- ------- ----------- ---------
node1 true    true        false
node2 true    true        false
2 entries were displayed.
```

19. Confirm connectivity between the cluster ports:

    `cluster ping-cluster local`

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

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

21. 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

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

Trademarks

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