



## **Cisco Nexus 3232C**

### Cluster and storage switches

NetApp  
April 05, 2024

# Table of Contents

- Cisco Nexus 3232C ..... 1
  - Overview ..... 1
  - Install hardware ..... 4
  - Configure software ..... 14
  - Migrate switches ..... 61
  - Replace switches ..... 153
  - Upgrade a Cisco Nexus 3232C storage switch ..... 194

# Cisco Nexus 3232C

## Overview

### Overview of installation and configuration for Cisco Nexus 3232c switches

Cisco Nexus 3232C switches can be used as cluster switches in your AFF or FAS cluster. Cluster switches allow you to build ONTAP clusters with more than two nodes.

#### Initial configuration overview

To initially configure a Cisco Nexus 3232c switch on systems running ONTAP, follow these steps:

1. [Complete Cisco Nexus 3232C cabling worksheet](#). The sample cabling worksheet provides examples of recommended port assignments from the switches to the controllers. The blank worksheet provides a template that you can use in setting up your cluster.
2. [Install a Cisco Nexus 3232C cluster switch in a NetApp cabinet](#). Install the Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet with the standard brackets that are included with the switch.
3. [Configure the 3232C cluster switch](#). Set up and configure the Cisco Nexus 3232C switch.
4. [Prepare to install NX-OS software and Reference Configuration File](#). Prepare to install the NX-OS software and the Reference Configuration File (RCF).
5. [Install the NX-OS software](#). Install the NX-OS software on the Nexus 3232C cluster switch.
6. [Install the Reference Configuration File \(RCF\)](#). 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.

#### Additional information

Before you begin installation or maintenance, be sure to review the following:

- [Configuration requirements](#)
- [Required documentation](#)
- [Smart Call Home requirements](#)

### Configuration requirements for Cisco Nexus 3232C switches

For Cisco Nexus 3232C switch installation and maintenance, be sure to review configuration and network requirements.

#### Configuration requirements

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.

#### Network requirements

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.

## Documentation requirements for Cisco Nexus 3232C switches

For Cisco Nexus 3232C switch installation and maintenance, be sure to review all recommended documentation.

### Switch documentation

To set up the Cisco Nexus 3232C switches, you need the following documentation from the [Cisco Nexus 3000 Series Switches Support](#) page.

Document title	Description
<i>Nexus 3000 Series Hardware Installation Guide</i>	Provides detailed information about site requirements, switch hardware details, and installation options.
<i>Cisco Nexus 3000 Series Switch Software Configuration Guides</i> (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.
<i>Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide</i> (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.
<i>Cisco Nexus 3000 Series NX-OS Command Reference Master Index</i>	Provides links to the various command references provided by Cisco.
<i>Cisco Nexus 3000 MIBs Reference</i>	Describes the Management Information Base (MIB) files for the Nexus 3000 switches.
<i>Nexus 3000 Series NX-OS System Message Reference</i>	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.
<i>Cisco Nexus 3000 Series NX-OS Release Notes</i> (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 3000 Series.

Document title	Description
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.

## ONTAP systems documentation

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 <i>Installation and Setup Instructions</i>	Describes how to install NetApp hardware.
ONTAP documentation	Provides detailed information about all aspects of the ONTAP releases.
<a href="#">Hardware Universe</a>	Provides NetApp hardware configuration and compatibility information.

## Rail kit and cabinet documentation

To install a 3232C Cisco switch in a NetApp cabinet, see the following hardware documentation.

Name	Description
<a href="#">42U System Cabinet, Deep Guide</a>	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.
<a href="#">Install a Cisco Nexus 3232C switch in a NetApp Cabinet</a>	Describes how to install a Cisco Nexus 3232C switch in a four-post NetApp cabinet.

## Smart Call Home requirements

To use Smart Call Home feature, review the following guidelines.

Smart Call Home monitors the hardware and software components on your network. When a critical system configuration occurs, it generates an email-based notification and raises an alert to all the recipients that are configured in your destination profile. To use Smart Call Home, you must configure a cluster network switch to communicate using email with the Smart Call Home system. In addition, 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, 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.

## Install hardware

### Complete Cisco Nexus 3232C cabling worksheet

If you want to document the supported platforms, download a PDF of this page and complete the cabling worksheet.

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

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	4x10GbE/4x25GbE or 40/100GbE node	1	4x10GbE/4x25GbE or 40/100GbE node
2	4x10GbE/4x25GbE or 40/100GbE node	2	4x10GbE/4x25GbE or 40/100GbE node
3	4x10GbE/4x25GbE or 40/100GbE node	3	4x10GbE/4x25GbE or 40/100GbE node
4	4x10GbE/4x25GbE or 40/100GbE node	4	4x10GbE/4x25GbE or 40/100GbE node
5	4x10GbE/4x25GbE or 40/100GbE node	5	4x10GbE/4x25GbE or 40/100GbE node
6	4x10GbE/4x25GbE or 40/100GbE node	6	4x10GbE/4x25GbE or 40/100GbE node
7	4x10GbE/4x25GbE or 40/100GbE node	7	4x10GbE/4x25GbE or 40/100GbE node
8	4x10GbE/4x25GbE or 40/100GbE node	8	4x10GbE/4x25GbE or 40/100GbE node

Cluster switch A		Cluster switch B	
9	4x10GbE/4x25GbE or 40/100GbE node	9	4x10GbE/4x25GbE or 40/100GbE node
10	4x10GbE/4x25GbE or 40/100GbE node	10	4x10GbE/4x25GbE or 40/100GbE node
11	4x10GbE/4x25GbE or 40/100GbE node	11	4x10GbE/4x25GbE or 40/100GbE node
12	4x10GbE/4x25GbE or 40/100GbE node	12	4x10GbE/4x25GbE or 40/100GbE node
13	4x10GbE/4x25GbE or 40/100GbE node	13	4x10GbE/4x25GbE or 40/100GbE node
14	4x10GbE/4x25GbE or 40/100GbE node	14	4x10GbE/4x25GbE or 40/100GbE node
15	4x10GbE/4x25GbE or 40/100GbE node	15	4x10GbE/4x25GbE or 40/100GbE node
16	4x10GbE/4x25GbE or 40/100GbE node	16	4x10GbE/4x25GbE or 40/100GbE node
17	4x10GbE/4x25GbE or 40/100GbE node	17	4x10GbE/4x25GbE or 40/100GbE node
18	4x10GbE/4x25GbE or 40/100GbE node	18	4x10GbE/4x25GbE or 40/100GbE node
19	40G/100GbE node 19	19	40G/100GbE node 19
20	40G/100GbE node 20	20	40G/100GbE node 20
21	40G/100GbE node 21	21	40G/100GbE node 21
22	40G/100GbE node 22	22	40G/100GbE node 22
23	40G/100GbE node 23	23	40G/100GbE node 23
24	40G/100GbE node 24	24	40G/100GbE node 24
25 through 30	Reserved	25 through 30	Reserved

Cluster switch A		Cluster switch B	
31	100GbE ISL to switch B port 31	31	100GbE ISL to switch A port 31
32	100GbE ISL to switch B port 32	32	100GbE 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	



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 through 30	Reserved	25 through 30	Reserved
31	100GbE ISL to switch B port 31	31	100GbE ISL to switch A port 31
32	100GbE ISL to switch B port 32	32	100GbE ISL to switch A port 32

## Configure the 3232C cluster switch

Follow this procedure to set up and configure the Cisco Nexus 3232C switch.

### What you'll need

- Access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.
- Applicable NX-OS version, downloaded from the [Cisco software download](#) page.
- Required cluster network and management network switch documentation.

See [Required documentation](#) for more information.

- Required controller documentation and ONTAP documentation.

[NetApp documentation](#)

- Applicable licenses, network and configuration information, and cables.
- Completed cabling worksheets.
- Applicable NetApp cluster network and management network RCFs, downloaded from the NetApp Support

Site at [mysupport.netapp.com](https://mysupport.netapp.com) for the switches that you receive. 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.

## Steps


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


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

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.

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.

Prompt	Response
Abort Auto Provisioning and continue with normal setup? (yes/no)	Respond with <b>yes</b> . The default is no.
Do you want to enforce secure password standard? (yes/no)	Respond with <b>yes</b> . 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 <b>yes</b> 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 <b>no</b> .
Configure read-only SNMP community string? (yes/no)	Respond with <b>no</b> . The default is no.
Configure read-write SNMP community string? (yes/no)	Respond with <b>no</b> . The default is no.
Enter the switch name.	The switch name is limited to 63 alphanumeric characters.

Prompt	Response
Continue with Out-of-band (mgmt0) management configuration? (yes/no)	Respond with <b>yes</b> (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 <b>yes</b> . At the IPv4 address of the default-gateway: prompt, enter your default_gateway.
Configure advanced IP options? (yes/no)	Respond with <b>no</b> . The default is no.
Enable the telnet service? (yes/no)	Respond with <b>no</b> . The default is no.
Enabled SSH service? (yes/no)	Respond with <b>yes</b> . The default is yes.  <div>  <p>SSH is recommended when using Cluster Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.</p> </div>
Enter the type of SSH key you want to generate (dsa/rsa/rsa1).	The default is <b>rsa</b> .
Enter the number of key bits (1024-2048).	Enter the number of key bits from 1024-2048.
Configure the NTP server? (yes/no)	Respond with <b>no</b> . The default is no.
Configure default interface layer (L3/L2):	Respond with <b>L2</b> . The default is L2.
Configure default switch port interface state (shut/noshut):	Respond with <b>noshut</b> . The default is noshut.
Configure CoPP system profile (strict/moderate/lenient/dense):	Respond with <b>strict</b> . 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 <b>no</b> at the prompt if you are satisfied with the configuration. Respond with <b>yes</b> if you want to edit your configuration settings.

Prompt	Response
Use this configuration and save it? (yes/no)	<p>Respond with <b>yes</b> to save the configuration. This automatically updates the kickstart and system images.</p> <div>  <p>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.</p> </div>

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 from the [Cisco software download](#) page.

### What's next?

[Prepare to install NX-OS and RCF.](#)

## Install a Cisco Nexus 3232C cluster switch in a NetApp cabinet

Depending on your configuration, you might need to install the Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet with the standard brackets that are included with the switch.

### What you'll need

- The initial preparation requirements, kit contents, and safety precautions in the [Cisco Nexus 3000 Series Hardware Installation Guide](#).
- For each switch, 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.
- 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.

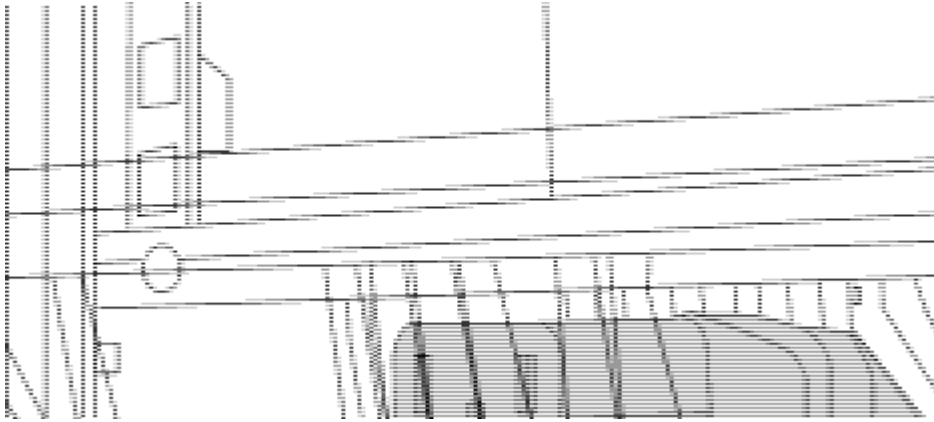
The pass-through panel kit is available from NetApp (part number X8784-R6).

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.

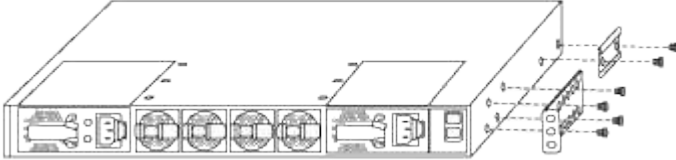
In this procedure, the blanking panel will be installed in U40.

- 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.

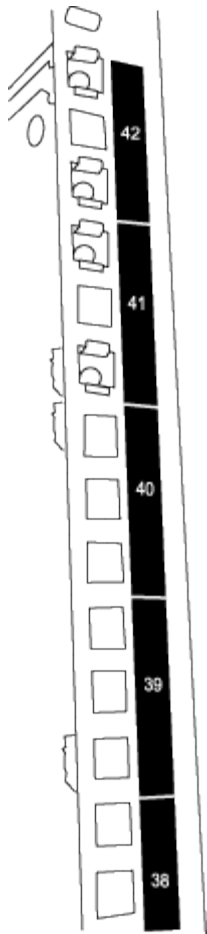


*(1) Female connector of the jumper cord.*

1. 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.



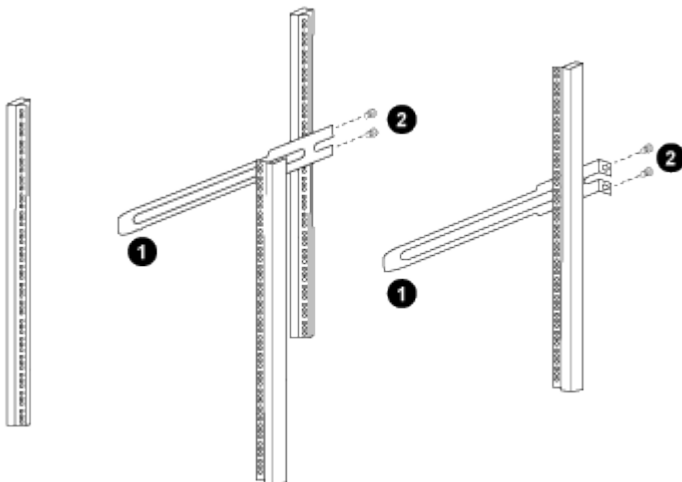
- b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.
  - c. Install the rear rack-mount bracket on the switch chassis.
  - d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.
2. Install the clip nuts in the square hole locations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



The two 3232C switches will always be mounted in the top 2U of the cabinet RU41 and 42.

3. 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.

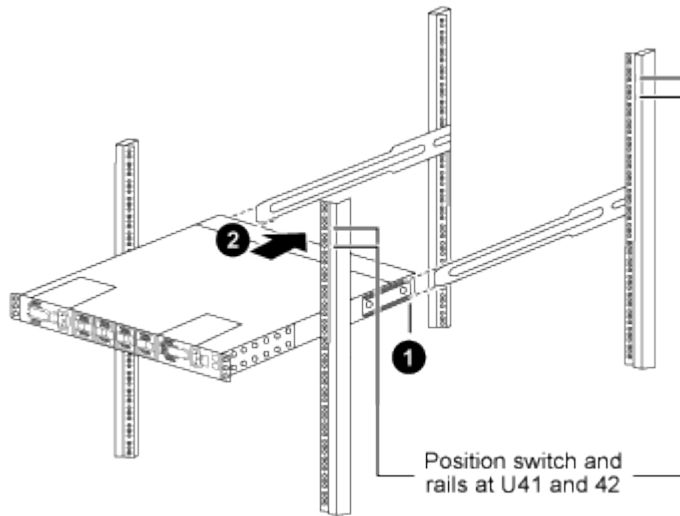
c. Repeat steps 4a and 4b at the RU41 locations on the cabinet.

4. 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.

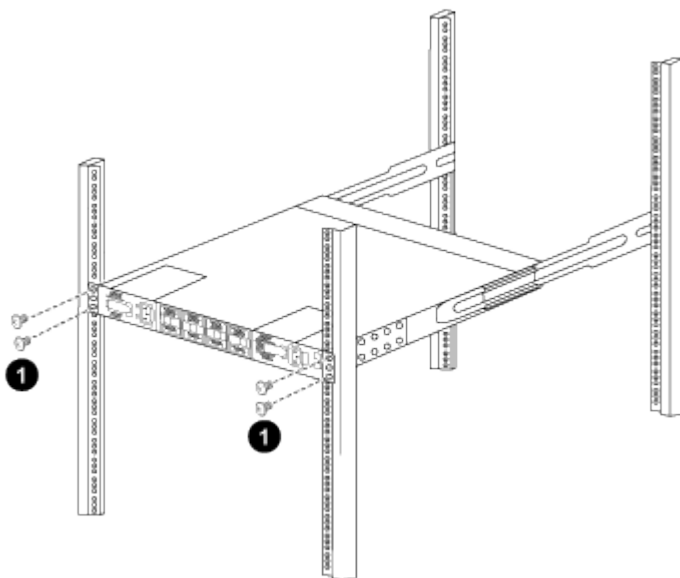
a. Position the back of the switch at RU41.



(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.

5. When the switches are installed, connect the jumper cords to the switch power inlets.
6. 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.

7. 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.

## Review cabling and configuration considerations

Before configuring your Cisco 3232C switch, review the following considerations.

### Support for NVIDIA CX6, CX6-DX, and CX7 Ethernet ports

If connecting a switch port to an ONTAP controller using NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX), or ConnectX-7 (CX7) NIC ports, you must hard-code the switch port speed.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

See the [Hardware Universe](#) for more information on switch ports.

## Configure software

### Prepare to install NX-OS software and Reference Configuration File (RCF)

Before you install the NX-OS software and the Reference Configuration File (RCF), follow this procedure.

#### About the examples



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.

### Switch and node nomenclature

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.

### About this task

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
```

### Show example

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

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

## Show example

```
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`

### Show example

```
cluster1::*> network interface show -vserver Cluster
```

Current Vserver Port	Home	Logical Current Is Interface	Status Admin/Oper	Network Address/Mask	Node
-----					
-----					
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`

## Show example

```
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`

### Show example

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

Vserver	Logical 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
```

## Show example

```
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
```

### Show example

```
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.

### Review requirements

#### What you'll need

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs or similar issues).
- [Cisco Ethernet switch page](#). Consult the switch compatibility table for the supported ONTAP and NX-OS versions.
- [Cisco Nexus 3000 Series Switches](#). Refer to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures.

### Install the software

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

Be sure to complete the procedure in [Prepare to install NX-OS and RCF](#), and then follow the steps below.

#### 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.

#### Show example

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.

## Show example

```
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:

```
show version
```

## Show example

```
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.

## Show example

```
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`

## Show example

```
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.



## Show example

```
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.

**Show example**

```
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.

**Show example**

```
cs2# show version module 1 epld

EPLD Device          Version
-----
MI    FPGA           0x12
IO    FPGA           0x12
```

## What's next?

[Install RCF config file](#)

## Install the Reference Configuration File (RCF)

Follow this procedure to 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. See the Knowledge Base article [How to clear configuration on a Cisco interconnect switch while retaining remote connectivity](#) for further information when upgrading your RCF.

### Review requirements

#### What you'll need

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs or similar issues).
- The current Reference Configuration File (RCF).
- A console connection to the switch, required when installing the RCF.
- [Cisco Ethernet switch page](#) Consult the switch compatibility table for the supported ONTAP and RCF versions. Note that there can be command dependencies between the command syntax in the RCF and that found in versions of NX-OS.
- [Cisco Nexus 3000 Series Switches](#). Refer to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures.

### Install the file

#### About the examples

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.

#### About this task

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

No operational inter-switch link (ISL) is needed during this procedure. This is by design because RCF version changes can affect ISL connectivity temporarily. To ensure non-disruptive cluster operations, the following procedure migrates all of the cluster LIFs to the operational partner switch while performing the steps on the target switch.

Be sure to complete the procedure in [Prepare to install NX-OS and RCF](#), and then follow the steps below.

### Steps

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

```
network device-discovery show
```

**Show example**

```
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
```

## Show example

```
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

Health	Health					Speed (Mbps)
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
```

### Show example

```
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
```

### Show example

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.92
NX3232C
    Serial Number: FOXXXXXXXXGS
    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: FOXXXXXXXXGD
    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.

### Show example

```
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.



### Show example

```
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
```

### Show example

```
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
```

### Show example

```
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 a copy of the current switch configuration by copying the output of the following command to a text file:

```
show running-config
```

8. Clean the configuration on switch cs2 and reboot the switch.



When updating or applying a new RCF, you must erase the switch settings and perform basic configuration. You must be connected to the switch serial console port to set up the switch again.

- a. Clean the configuration:

### Show example

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n)  [n]  y
```

- b. Reboot the switch:

### Show example

```
(cs2)# reload

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

9. Perform a basic setup of the switch. See [Configure the 3232C cluster switch](#) for details.

10. 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.

#### Show example

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)...
```

11. 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.

#### Show example

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
```

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

## Show example

```
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.

13. 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.

14. 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
```

15. 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
```

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

### Show example

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands  
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

17. 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
```

## Show example

```
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

Health	Health				Speed (Mbps)	
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).



## Show example

```
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: FOXXXXXXXXGD
    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: FOXXXXXXXXGS
    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.

```



It can take up to 5 minutes for the cluster nodes to report as healthy.

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

#### Show example

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

```

19. 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
```

## Show example

```
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::*>				

## 20. Verify that the cluster is healthy:

```
cluster show
```

### Show example

```
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::*>
```

21. Repeat Steps 7 to 15 on switch cs1.
22. Enable auto-revert on the cluster LIFs.

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

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

### Show example

```
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
```

### Show example

```
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 -role cluster
```

## Show example

```
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::*>				

If any cluster LIFS have not returned to their home ports, revert them manually: `network interface revert -vserver vservice_name -lif lif_name`

## 26. Verify that the cluster is healthy:

```
cluster show
```

### Show example

```
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::*>
```

27. Ping the remote cluster interfaces to verify connectivity:

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

## Show example

```
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)
```

## Ethernet Switch Health Monitoring log collection

You can use the log collection feature to collect switch-related log files in ONTAP. The Ethernet switch health monitor (CSHM) is responsible for ensuring the operational health



of Cluster and Storage network switches and collecting switch logs for debugging purposes. This procedure guides you through the process of setting up and starting the collection of detailed **Support** logs from the switch and starts an hourly collection of **Periodic** data that is collected by AutoSupport.

#### Before you begin

- Verify that you have set up your environment using the Cisco 3232C cluster switch **CLI**.
- Switch health monitoring must be enabled for the switch. Verify this by ensuring the `Is Monitored:` field is set to **true** in the output of the `system switch ethernet show` command.

#### Steps

1. Create a password for the Ethernet switch health monitor log collection feature:

```
system switch ethernet log setup-password
```

#### Show example

```
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
Would you like to specify a user other than admin for log
collection? {y|n}: n

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
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. To start log collection, run the following command, replacing **DEVICE** with the switch used in the previous command. This starts both types of log collection: the detailed **Support** logs and an hourly collection of **Periodic** data.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

### Show example

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

Wait for 10 minutes and then check that the log collection completes:

```
system switch ethernet log show
```



If any of these commands return an error or if the log collection does not complete, contact NetApp support.

### Troubleshooting

If you encounter any of the following error statuses reported by the log collection feature (visible in the output of `system switch ethernet log show`), try the corresponding debug steps:

Log collection error status	Resolution
<b>RSA keys not present</b>	Regenerate ONTAP SSH keys. Contact NetApp support.
<b>switch password error</b>	Verify credentials, test SSH connectivity, and regenerate ONTAP SSH keys. Review the switch documentation or contact NetApp support for instructions.
<b>ECDSA keys not present for FIPS</b>	If FIPS mode is enabled, ECDSA keys need to be generated on the switch before retrying.
<b>pre-existing log found</b>	Remove the previous log collection file on the switch.

<b>switch dump log error</b>	Ensure the switch user has log collection permissions. Refer to the prerequisites above.
------------------------------	--

## Configure SNMPv3

Follow this procedure to configure SNMPv3, which supports Ethernet switch health monitoring (CSHM).

### About this task

The following commands configure an SNMPv3 username on Cisco 3232C switches:

- For **no authentication**: `snmp-server user SNMPv3_USER NoAuth`
- For **MD5/SHA authentication**: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- For **MD5/SHA authentication with AES/DES encryption**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 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 CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

### Steps

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

```
show snmp user
```

## Show example

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1) (Config)# show snmp user

-----
-----
                        SNMP USERS
-----
-----

User                Auth                Priv(enforce)    Groups
acl_filter
-----
-----
admin               md5                des(no)          network-admin
SNMPv3User          md5                aes-128(no)      network-operator
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

User                Auth                Priv
-----
-----

(sw1) (Config)#
```

## 2. Set up the SNMPv3 user on the ONTAP side:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

### Show example

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-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 CSHM to monitor with the new SNMPv3 user:

```
system switch ethernet show-all -device "sw1" -instance
```

## Show example

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N3K-C3232C
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

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

```
system switch ethernet polling-interval show
```

### Show example

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

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N3K-C3232C
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

## Migrate switches

### Migration requirements for Cisco Nexus 3232C cluster switches

Before you migrate to Cisco Nexus 3232C cluster switches. review the configuration information, port connections, and cabling requirements.

#### CN1610 migrate requirements

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](#).

## CN5596 requirements

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](#).

## 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.

### Review requirements

Before migration, be sure to review [Migration requirements](#).



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

If necessary, refer to the following for more information:

- [NetApp CN1601 and CN1610 description page](#)
- [Cisco Ethernet Switch description page](#)
- [Hardware Universe](#)

### Migrate the switches

#### About the examples

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 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.

### Step 1: Prepare for migration

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
```

### Show example

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
```

Node	Local Port	Discovered 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
```

## Show example

```
cluster::*> network port show -role cluster
(network port show)
```

Node: n1

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

-----

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n2

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

-----

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	
e0d	cluster	cluster	up	9000	auto/10000	-	

8 entries were displayed.

b. Display information about the logical interfaces:

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

## Show example

```
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
true      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

8 entries were displayed.
```

c. Display information about the discovered cluster switches:

```
system cluster-switch show
```

### Show example

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
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 -vserver vserver-name -lif lif-name -source-node  
source-node-name destination-node destination-node-name -destination-port  
destination-port-name
```

### Show example

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
```

## Show example

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current  Current  Is
Vserver Interface Admin/Oper Address/Mask Node      Port      Is
Home
-----
Cluster
true      n1_clus1    up/up      10.10.0.1/24  n1        e0a
false     n1_clus2    up/up      10.10.0.2/24  n1        e0a
false     n1_clus3    up/up      10.10.0.3/24  n1        e0d
true      n1_clus4    up/up      10.10.0.4/24  n1        e0d
true      n2_clus1    up/up      10.10.0.5/24  n2        e0a
false     n2_clus2    up/up      10.10.0.6/24  n2        e0a
false     n2_clus3    up/up      10.10.0.7/24  n2        e0d
true      n2_clus4    up/up      10.10.0.8/24  n2        e0d

8 entries were displayed.
```

## Step 2: Replace cluster switch CL2 with C2

1. 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
```



### Show example

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
```

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

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

## Show example

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)
```

3. 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](#).

#### Show example

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)#
```

4. 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](#).

#### Show example

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
```

5. 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.

6. 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.

7. 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.

For more information on Cisco commands, see the guides listed in the [Cisco Nexus 3000 Series NX-OS Command References](#).

#### Show example

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) #
```

8. 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](#).

#### Show example

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) #
```

9. 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.

## Show example

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
```

10. 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.

### Show example

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)
```

11. 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
```

### Show example

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
```

12. 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
```

### Show 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
```

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

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

### Show example

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
true      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

8 entries were displayed.
```

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

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

**Show example**

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

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Domain      Health      Admin/Open  Status      Health
-----  -
e0a    cluster  cluster    up    9000  auto/10000    -
e0b    cluster  cluster    up    9000  auto/10000    -
e0c    cluster  cluster    up    9000  auto/10000    -
e0d    cluster  cluster    up    9000  auto/10000    -
Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Domain      Health      Admin/Open  Status      Health
-----  -
e0a    cluster  cluster    up    9000  auto/10000    -
e0b    cluster  cluster    up    9000  auto/10000    -
e0c    cluster  cluster    up    9000  auto/10000    -
e0d    cluster  cluster    up    9000  auto/10000    -

8 entries were displayed.
```

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

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



## Show example

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)
```

16. Migrate the LIFs that are associated with the first CN1610 switch CL1:

```
network interface migrate -vserver cluster -lif lif-name -source-node node-name
```

**Show example**

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
```

**Step 3: Replace cluster switch CL1 with C1**

1. Verify the cluster's status:

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

### Show example

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
false      n1_clus1    up/up      10.10.0.1/24  n1       e0b
true       n1_clus2    up/up      10.10.0.2/24  n1       e0b
true       n1_clus3    up/up      10.10.0.3/24  n1       e0c
false      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.
```

2. 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
```

### Show example

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
```

3. 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](#).

#### Show example

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#
```

4. 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.

5. 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.

6. 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](#).

## Show example

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.
```

7. 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](#).

### Show example

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.
```

8. 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](#).

## Show example

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

9. 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
```

### Show example

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
```

10. Verify the status of the cluster node port:

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



## Show example

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

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status                               Admin/Open  Status  Health
-----
-----
e0a   cluster  cluster    up    9000  auto/10000    -       -
e0b   cluster  cluster    up    9000  auto/10000    -       -
e0c   cluster  cluster    up    9000  auto/10000    -       -
e0d   cluster  cluster    up    9000  auto/10000    -       -

Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status                               Admin/Open  Status  Health
-----
-----
e0a   cluster  cluster    up    9000  auto/10000    -       -
e0b   cluster  cluster    up    9000  auto/10000    -       -
e0c   cluster  cluster    up    9000  auto/10000    -       -
e0d   cluster  cluster    up    9000  auto/10000    -       -

8 entries were displayed.
```

## Step 4: Complete the procedure

1. 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
```

### Show example

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
```

2. Verify that the interface is now home:

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

### Show example

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
true      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

8 entries were displayed.
```

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

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

## Show example

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)
```

4. Expand the cluster by adding nodes to the Nexus 3232C cluster switches.

5. 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

## Show example

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
```

Node	Local Port	Discovered 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
n2	/cdp			
	e0d	C1	Ethernet1/1/2	N3K-C3232C
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
n3	/cdp			
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
	e4a	C1	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4e	C2	Ethernet1/7	N3K-C3232C
	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.

```

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

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

#### Show example

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

```

7. Verify that the proper cluster switches are monitored:

```
system cluster-switch show
```

## Show example

The following example shows cluster switches C1 and C2 are being monitored:

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

Switch Model	Type	Address
-----		
C1 NX3232C	cluster-network	10.10.1.103
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 NX3232C	cluster-network	10.10.1.104
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.

8. 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
```

## Show example

```
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.

9. 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 Nexus 5596 cluster switch to a Cisco Nexus 3232C cluster switch

Follow this procedure to migrate an existing Cisco Nexus 5596 cluster switches in a cluster with Nexus 3232C cluster switches.

## Review requirements

Before migration, be sure to review [Migration requirements](#).



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

For more information, see:

- [Cisco Ethernet Switch description page](#)
- [Hardware Universe](#)

## Migrate the switch

### About the examples

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.

## Scenarios

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.
  - 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.

### Step 1: Prepare for migration

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
```

### Show example

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
```

Node	Local Port	Discovered 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
```

## Show example

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

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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
```

### Show example

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)
Current Is Logical Status Network Current
Vserver Is Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e0a      true  n1_clus1  up/up    10.10.0.1/24  n1
e0b      true  n1_clus2  up/up    10.10.0.2/24  n1
e0c      true  n1_clus3  up/up    10.10.0.3/24  n1
e0d      true  n1_clus4  up/up    10.10.0.4/24  n1
e0a      true  n2_clus1  up/up    10.10.0.5/24  n2
e0b      true  n2_clus2  up/up    10.10.0.6/24  n2
e0c      true  n2_clus3  up/up    10.10.0.7/24  n2
e0d      true  n2_clus4  up/up    10.10.0.8/24  n2
8 entries were displayed.
```

### c. Display information about the discovered cluster switches:

```
system cluster-switch show
```



## Show example

The following example shows the active cluster switches:

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

Switch Model	Type	Address
CL1 NX5596	cluster-network	10.10.1.101
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 NX5596	cluster-network	10.10.1.102
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 vservice-name -lif lif-name -source-node
source-node-name - destination-node node-name -destination-port destination-
port-name
```

#### Show example

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
```

## Show example

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
e0a          n1_clus1    up/up      10.10.0.1/24      n1
true
e0a          n1_clus2    up/up      10.10.0.2/24      n1
false
e0d          n1_clus3    up/up      10.10.0.3/24      n1
false
e0d          n1_clus4    up/up      10.10.0.4/24      n1
true
e0a          n2_clus1    up/up      10.10.0.5/24      n2
true
e0a          n2_clus2    up/up      10.10.0.6/24      n2
false
e0d          n2_clus3    up/up      10.10.0.7/24      n2
false
e0d          n2_clus4    up/up      10.10.0.8/24      n2
true
8 entries were displayed.
```

## Step 2: Configure ports

1. 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
```

### Show example

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
```

2. Ping the remote cluster interfaces and perform an RPC server check:

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

## Show example

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)
```

3. 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](#).

#### Show example

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) #
```

4. 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](#).

#### Show example

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
```

5. 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.

6. 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.

7. 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](#).

#### Show example

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) #
```

8. 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](#).

### Show example

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)
```

9. Verify that interfaces eth1/45-48 already have `channel-group 1 mode active` in their running configuration.
10. 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
```

### Show example

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
```

11. On all nodes, revert all of the migrated cluster interconnect LIFs connected to C2:

```
network interface revert -vserver Cluster -lif lif-name
```



### Show example

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
```

12. Verify all the cluster interconnect ports are now reverted to their home:

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

### Show example

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
e0a      n1_clus1      up/up      10.10.0.1/24      n1
      true
e0b      n1_clus2      up/up      10.10.0.2/24      n1
      true
e0c      n1_clus3      up/up      10.10.0.3/24      n1
      true
e0d      n1_clus4      up/up      10.10.0.4/24      n1
      true
e0a      n2_clus1      up/up      10.10.0.5/24      n2
      true
e0b      n2_clus2      up/up      10.10.0.6/24      n2
      true
e0c      n2_clus3      up/up      10.10.0.7/24      n2
      true
e0d      n2_clus4      up/up      10.10.0.8/24      n2
      true
8 entries were displayed.
```

### 13. Verify that the clustered ports are connected:

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

## Show example

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.
```

14. Ping the remote cluster interfaces and perform an RPC server check:

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

## Show example

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)
```

15. On each node in the cluster, migrate the interfaces associated with the first Nexus 5596 switch, CL1, to be replaced:

```
network interface migrate -vserver vservice-name -lif lif-name -source-node
source-node-name -destination-node destination-node-name -destination-port
destination-port-name
```

#### Show example

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
```

16. Verify the cluster's status:

```
network interface show
```

## Show example

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
```

Current Is	Logical	Status	Network	Current
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.				
-----				

17. 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
```

### Show example

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
```

18. 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](#).

### Show example

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#
```

19. 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.

20. 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.

21. 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](#).



### Show example

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.
```

22. 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](#).

### Show example

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
```

23. 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

### Show example

```
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)
```

24. On all nodes, bring up all the cluster interconnect ports connected to the new 3232C switch C1:

```
network port modify
```

### Show example

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
```

25. Verify the status of the cluster node port:

```
network port show
```

## Show example

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

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

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.
```

26. On all nodes, revert the specific cluster LIFs to their home ports:

```
network interface revert -server Cluster -lif lif-name
```

### Show example

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
```

### 27. Verify that the interface is home:

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

## Show example

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)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e0a n1_clus1 up/up 10.10.0.1/24 n1
true
e0b n1_clus2 up/up 10.10.0.2/24 n1
true
e0c n1_clus3 up/up 10.10.0.3/24 n1
true
e0d n1_clus4 up/up 10.10.0.4/24 n1
true
e0a n2_clus1 up/up 10.10.0.5/24 n2
true
e0b n2_clus2 up/up 10.10.0.6/24 n2
true
e0c n2_clus3 up/up 10.10.0.7/24 n2
true
e0d n2_clus4 up/up 10.10.0.8/24 n2
true
8 entries were displayed.
```

28. Ping the remote cluster interfaces and perform an RPC server check:

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

## Show example

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)
```

29. 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.

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

## Show example

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

Node	Local Port	Discovered 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
```

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

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 Model	Type	Address
-----		
C1 NX3232C	cluster-network	10.10.1.103
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 NX3232C	cluster-network	10.10.1.104
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 NX5596	cluster-network	10.10.1.101
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 NX5596	cluster-network	10.10.1.102
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.
```

30. 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
```

**Show example**

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

**Step 3: Complete the procedure**

1. Verify that the proper cluster switches are monitored:

```
system cluster-switch show
```

## Show example

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

Switch Model	Type	Address
-----		
C1 NX3232C	cluster-network	10.10.1.103
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 NX3232C	cluster-network	10.10.1.104
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.

2. 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
```

## Show example

```
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.

3. 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 two-node switchless cluster to a cluster with Cisco Nexus 3232C cluster switches

If you have a two-node *switchless* cluster, you can migrate to a two-node *switched* cluster that includes Cisco Nexus 3232C cluster network switches. This is a nondisruptive procedure.

### Review requirements

#### Migration requirements

Before migration, be sure to review [Migration requirements](#).

#### What you'll need

Ensure that:

- Ports are available for node connections. The cluster switches use the Inter-Switch Link (ISL) ports e1/31-32.
- You have 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 supported QSFP/ 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.
- The configurations are properly set up and functioning.

The two nodes must be connected and functioning in a two-node switchless cluster setting.

- All cluster ports are in the **up** state.
- The Cisco Nexus 3232C cluster switch are supported.
- The existing cluster network configuration has 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

### Migrate the switches

#### About the examples

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.

### Step 1: Display and migrate physical and logical ports

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
```



## Show example

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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
```

### Show example

```
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
e4a      n1_clus1    up/up      10.10.0.1/24  n1
true
e4e      n1_clus2    up/up      10.10.0.2/24  n1
true
e4a      n2_clus1    up/up      10.10.0.3/24  n2
true
e4e      n2_clus2    up/up      10.10.0.4/24  n2
true

4 entries were displayed.
```

- c. Verify that switchless cluster detection is enabled using the advanced privilege command:

```
network options detect-switchless-cluster show`
```

### Show example

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](#).

#### Show example

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](#).

## Show example

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](#).

## Show example

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
```

### Show example

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 vservice-name -lif lif-name source-node  
source-node-name -destination-port destination-port-name
```

### Show example

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
```

## Step 2: Shut down the reassigned LIFs and disconnect the cables

1. Verify the cluster interfaces have successfully migrated:

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

### Show example

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)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4e n1_clus1 up/up 10.10.0.1/24 n1
false
e4e n1_clus2 up/up 10.10.0.2/24 n1
true
e4e n2_clus1 up/up 10.10.0.3/24 n2
false
e4e n2_clus2 up/up 10.10.0.4/24 n2
true
4 entries were displayed.
```

2. 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
```

### Show example

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
```

3. Ping the remote cluster interfaces and perform an RPC server check:

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

## Show example

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)
```

### 4. 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.

## Step 3: Enable the cluster ports

### 1. 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.

### 2. 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](#).



### Show example

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
```

3. Enable the first cluster port, e4a, on each node:

```
network port modify -node node-name -port port-name -up-admin true
```

### Show example

```
cluster::*> network port modify -node n1 -port e4a -up-admin true
cluster::*> network port modify -node n2 -port e4a -up-admin true
```

4. Verify that the clusters are up on both nodes:

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

### Show example

```
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.
```

5. For each node, revert all of the migrated cluster interconnect LIFs:

```
network interface revert -vserver cluster -lif lif-name
```

### Show example

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
```

6. 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.

#### Show example

```
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.
```

#### Step 4: Enable the reassigned LIFs

1. Display the cluster port connectivity on each node:

```
network device-discovery show
```

### Show example

```
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

2. 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
```

### Show example

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
```

3. Shut down cluster ports clus2 LIF on both nodes:

```
network port modify
```

### Show example

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
```

#### 4. Verify the cluster LIF status:

```
network interface show
```

##### Show example

```
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.
```

#### 5. 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.

#### 6. 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.

#### 7. Enable all node-facing ports on C2.

### Show example

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
```

8. Enable the second cluster port, e4e, on each node:

```
network port modify
```

### Show example

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*s
```

9. For each node, revert all of the migrated cluster interconnect LIFs: `network interface revert`

### Show example

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
```

10. 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.

### Show example

```
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
e4a      n1_clus1    up/up      10.10.0.1/24      n1
      true
e4e      n1_clus2    up/up      10.10.0.2/24      n1
      true
e4a      n2_clus1    up/up      10.10.0.3/24      n2
      true
e4e      n2_clus2    up/up      10.10.0.4/24      n2
      true
4 entries were displayed.
```

11. Verify that all of the cluster interconnect ports are in the up state:

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

12. Display the cluster switch port numbers through which each cluster port is connected to each node:

```
network device-discovery show
```

### Show example

```
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
```

13. Display discovered and monitored cluster switches:

```
system cluster-switch show
```

### Show example

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

Switch Model	Type	Address
-----		
C1 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	cluster-network	10.10.1.101
C2 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.	cluster-network	10.10.1.102

14. Verify that switchless cluster detection changed the switchless cluster option to disabled:

```
network options switchless-cluster show
```

15. Ping the remote cluster interfaces and perform an RPC server check:

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



### Show example

```
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)
```

16. 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
```

## Show example

```
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.

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 switches

## Replace a Cisco Nexus 3232C cluster switch

Follow these steps to replace a defective Cisco Nexus 3232C switch in a cluster. This is a non-disruptive procedure.

### Review requirements

#### What you'll need

Make sure that the existing cluster and network configuration has the following characteristics:

- The Nexus 3232C cluster infrastructure are 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) are in the **up** state and are not migrated.

The replacement Cisco Nexus 3232C switch has the following characteristics:

- Management network connectivity is functional.
- Console access to the replacement switch is in place.
- The appropriate RCF and NX-OS operating system image is loaded onto the switch.
- Initial customization of the switch is complete.

### For more information

See the following:

- [Cisco Ethernet Switch description page](#)
- [Hardware Universe](#)

## Replace the switch

### About this task

This replacement 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.

### About the examples

This replacement 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 replacement 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.

#### Step 1: Display and migrate the cluster ports to switch

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
```

### Show example

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

Node	Local Port	Discovered 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
n2	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3232C
	e0b	CL2	Ethernet1/1/3	N3K-C3232C
	e0c	CL2	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

3. Determine the administrative or operational status for each cluster interface.

a. Display the network port attributes:

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

## Show example

```
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

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
e4e         Cluster      Cluster      up    9000 auto/40000 -

```

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

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

## Show example

```
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			

c. Display the discovered cluster switches:

```
system cluster-switch show
```



### Show example

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: None
    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: None
    Software Version: Cisco Nexus Operating System (NX-OS)
    Software, Version 7.0(3)I6(1)
    Version Source: CDP
```

4. 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](https://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](#)

5. Migrate the cluster LIFs to the physical node ports connected to the replacement switch C2:

```
network interface migrate -vserver vservice-name -lif lif-name -source-node
node-name -destination-node node-name -destination-port port-name
```

### Show example

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 -destination-
node n4 -destination-port e4a
```

6. Verify the status of the cluster ports and their home designations:

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

## Show example

```
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			

## 7. 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
```

### Show example

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
```

8. Ping the remote cluster interfaces and perform an RPC server check:

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

## Show example

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)
```

## Step 2: Migrate ISLs to switch CL1 and C2

1. 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](#).

### Show example

```
(CL1)# configure
(CL1) (Config)# interface e1/31-32
(CL1) (config-if-range)# shutdown
(CL1) (config-if-range)# exit
(CL1) (Config)# exit
(CL1)#
```

2. Remove all the cables attached to the cluster switch CL2 and reconnect them to the replacement switch C2 for all the nodes.
3. 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.
4. 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](#).

### Show example

```
(CL1)# configure
(CL1) (Config)# interface e1/31-32
(CL1) (config-if-range)# no shutdown
(CL1) (config-if-range)# exit
(CL1) (Config)# exit
(CL1)#
```

5. 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:

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

6. 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](#).

### Show example

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)
```

7. 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
```

### Show example

```
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
```

### Step 3: Revert all LIFs to originally assigned ports

1. Revert all the migrated cluster interconnect LIFs on all the nodes:

```
network interface revert -vserver cluster -lif lif-name
```



### Show example

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
```

2. Verify that the cluster interconnect ports are now reverted to their home:

```
network interface show
```

## Show example

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			

### 3. Verify that the cluster ports are connected:

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

## Show example

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

-----

-----

e4a	Cluster	Cluster		up	9000	auto/40000	-
-----	---------	---------	--	----	------	------------	---

e4e	Cluster	Cluster		up	9000	auto/40000	-
-----	---------	---------	--	----	------	------------	---

-							
---	--	--	--	--	--	--	--

4. Ping the remote cluster interfaces and perform an RPC server check:

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

## Show example

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)
```

#### **Step 4: Verify all ports and LIF are correctly migrated**

1. 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

## Show example

```
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

```
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
-----							
-----							
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	
-----								
-----								
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	
-----								
-----								
e4a	Cluster	Cluster		up	9000	auto/40000	-	
e4e	Cluster	Cluster		up	9000	auto/40000	-	

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			

cluster::\*> **system cluster-switch show**

Switch	Type	Address
Model		
-----	-----	-----
CL1	cluster-network	10.10.1.101
NX3232C		
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
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: None		
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: None
```

```
Software Version: Cisco Nexus Operating System (NX-OS)
```

```
Software, Version 7.0(3)I6(1)
```

```
Version Source: CDP 3 entries were displayed.
```

2. Delete the replaced cluster switch CL2 if it has not been removed automatically:

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

3. Verify that the proper cluster switches are monitored:

```
system cluster-switch show
```

### Show example

The following example shows the cluster switches are monitored because the Is Monitored state is true.

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

Switch Model	Type	Address
CL1 NX3232C	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		

4. 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
```

### Show example

```
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.

5. 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 storage switch

Follow these steps to replace a defective Cisco Nexus 3232C storage switch. This is a non-disruptive procedure.

### Review requirements

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.

### Replace the switch

This procedure replaces the second Nexus 3232C storage switch S2 with the new 3232C switch NS2. The two nodes are node1 and node2.

#### Step 1: Confirm the switch to be replaced is S2

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
```

Show example

```
storage::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed	State	Status	VLAN
				(Gb/s)			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
```

### Show example

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

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

### Show example

```
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
```

### Step 2: Configure cabling

1. Verify the shelf ports in the storage system:

```
storage shelf port show -fields remote-device,remote-port
```

### Show example

```
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   -            -
```

2. Remove all cables attached to storage switch S2.
3. Reconnect all cables to the replacement switch NS2.

### Step 3: Verify all device configurations on switch NS2

1. Verify the health status of the storage node ports:

storage port show -port-type ENET

Show example

```
storage::*> storage port show -port-type ENET
```

VLAN				Speed		
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						

2. Verify that both switches are available:

network device-discovery show



### Show example

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

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

### 3. Verify the shelf ports in the storage system:

```
storage shelf port show -fields remote-device,remote-port
```

### Show example

```
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
```

4. 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 3232C cluster switches with switchless connections

You can migrate from a cluster with a switched cluster network to one where two nodes are directly connected for ONTAP 9.3 and later.

### Review requirements

#### Guidelines

Review the following guidelines:

- Migrating 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.
- You cannot use the switchless cluster interconnect feature with more than two nodes.
- 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.

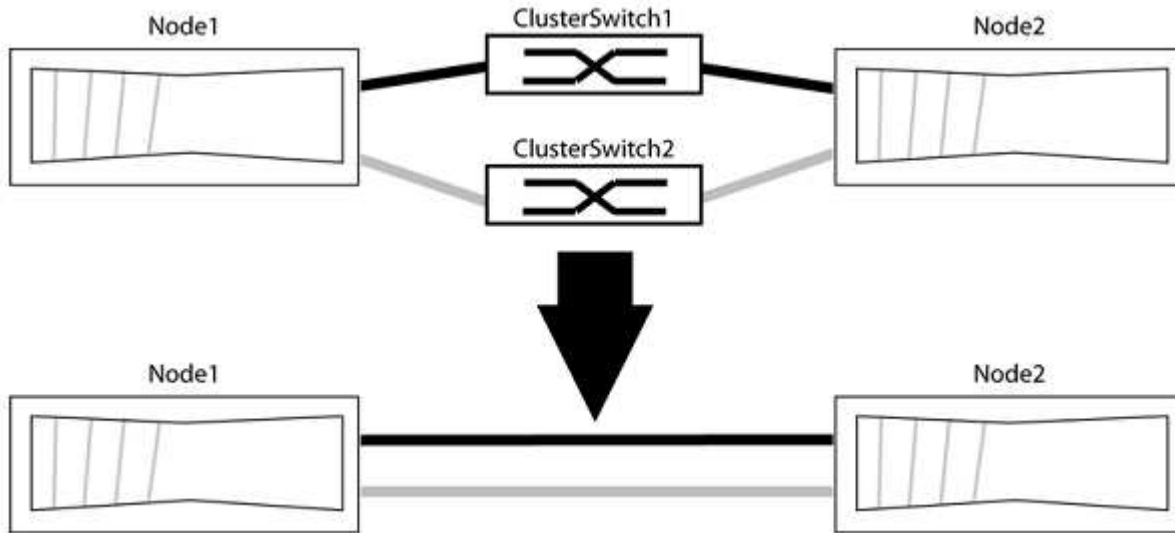
#### What you'll need

- A healthy cluster that consists of two nodes connected by cluster switches. The nodes must be running the same ONTAP release.
- Each node with the required number of dedicated cluster ports, which provide redundant cluster interconnect connections to support your system configuration. For example, there are two redundant ports for a system with two dedicated cluster interconnect ports on each node.

### Migrate the switches

#### 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.



### About the examples

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.

#### Step 1: Prepare for migration

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
```

#### Show example

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 NetApp 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:

#### Show example

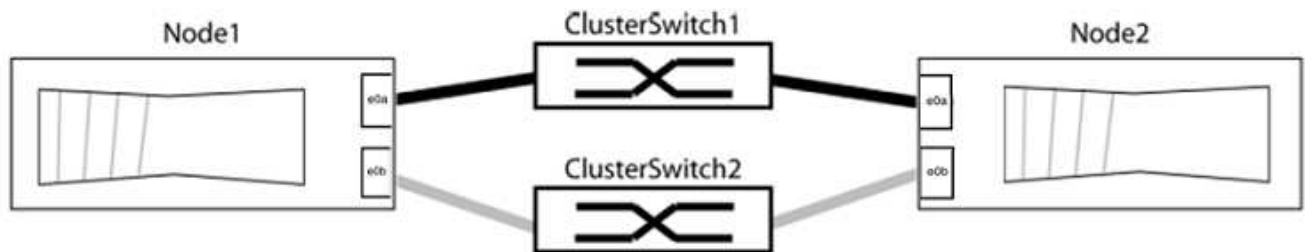
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

### Step 2: Configure ports and cabling

1. 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.
2. 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.

### Show 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.
```

3. 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
```

### Show 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 *
```

#### 4. Disable auto-revert for the cluster LIFs:

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

#### 5. 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.

### Show example

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.
```

#### 6. Verify the cluster connectivity:

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

7. Verify that the cluster is healthy:

```
cluster ring show
```

All units must be either master or secondary.

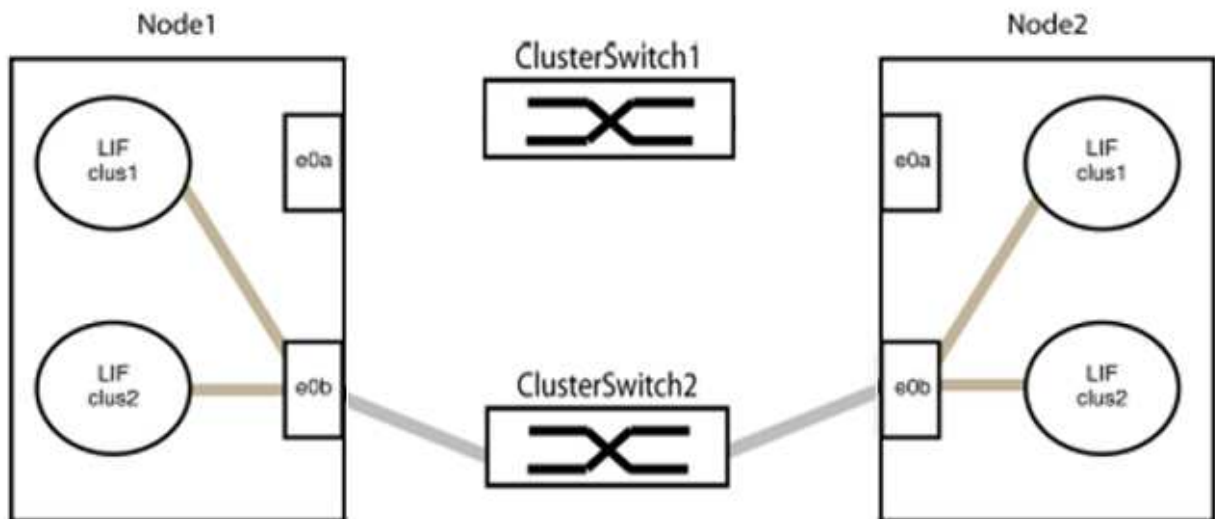
8. Set up the switchless configuration for the ports in group 1.



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:

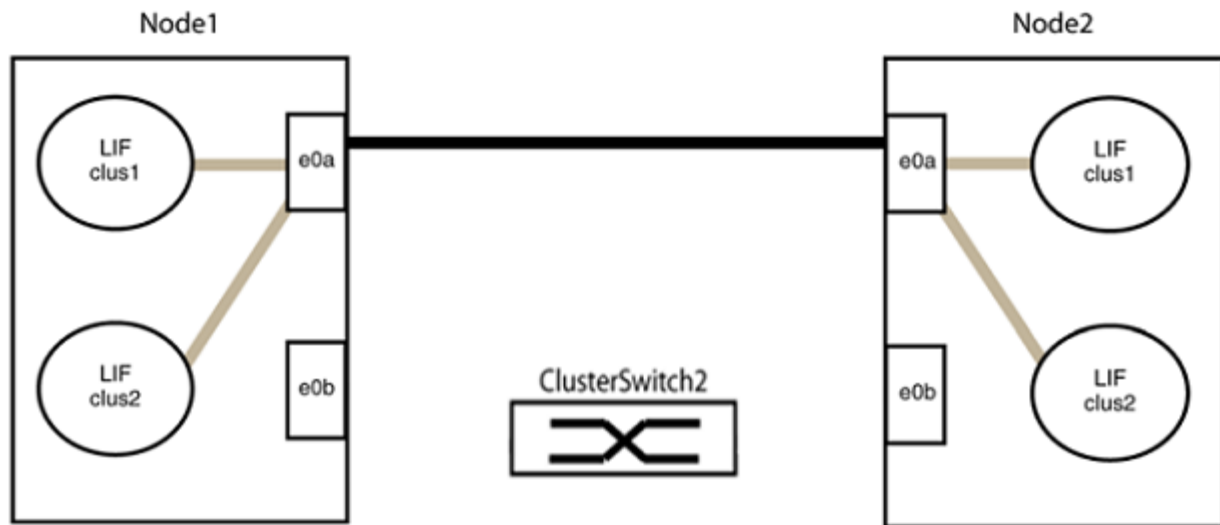


b. Cable the ports in group1 back-to-back.

In the following example, "e0a" on node1 is connected to "e0a" on node2:

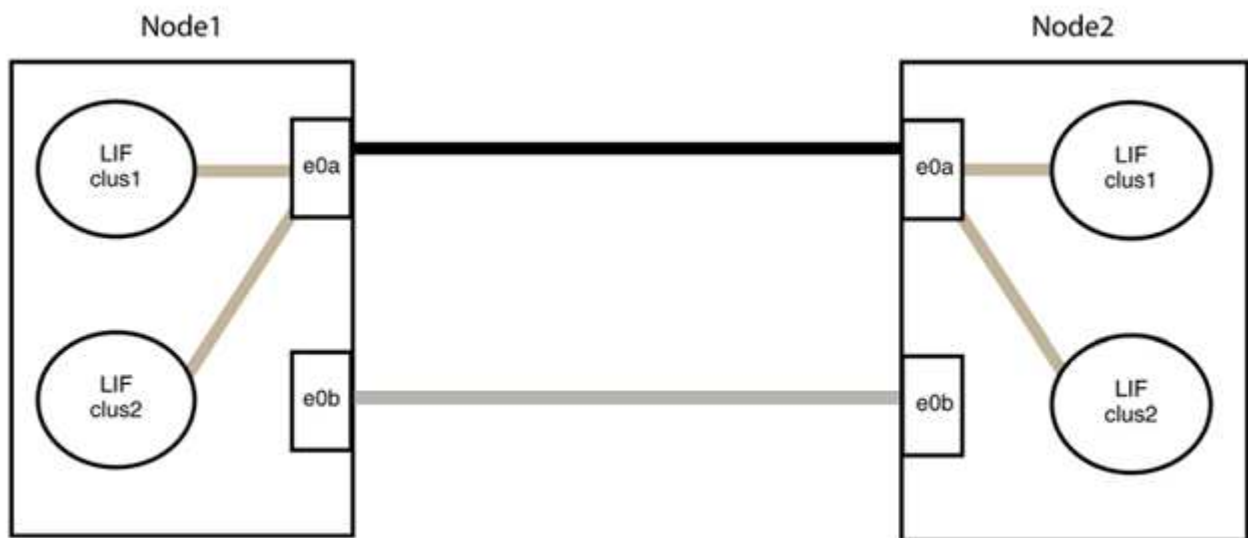






b. Cable the ports in group2 back-to-back.

In the following example, "e0a" on node1 is connected to "e0a" on node2 and "e0b" on node1 is connected to "e0b" on node2:



### Step 3: Verify the configuration

1. Verify that the ports on both nodes are correctly connected:

```
network device-discovery show -port cluster_port
```

## Show example

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.
```

### 2. Re-enable auto-revert for the cluster LIFs:

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

### 3. Verify that all LIFs are home. This might take a few seconds.

```
network interface show -vserver Cluster -lif lif_name
```

### Show example

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 from the local node:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Check the cluster status of the nodes from the system console of either node:

```
cluster show
```

### Show example

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.
```

5. Confirm connectivity between the cluster ports:

```
cluster ping-cluster local
```

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

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

For more information, see [NetApp KB Article 1010449: How to suppress automatic case creation during scheduled maintenance windows](#).

7. Change the privilege level back to admin:

```
set -privilege admin
```

## Upgrade a Cisco Nexus 3232C storage switch

Follow these steps to upgrade the Cisco NX-OS software and reference configuration files (RCF) on Cisco Nexus 3232C switches.

### Review requirements

#### What you'll need

Ensure that the following conditions exist before you upgrade the NX-OS software and RCFs on the storage switch:

- The switch is fully functioning (there should be no errors in the logs or similar issues).
- You 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 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.

### Replace the switch

#### About the examples

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 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 procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated. The command outputs might vary depending on different releases of ONTAP.

#### Step 1: Check the health status of switches and ports

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
```

**Show example**

```
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
```

### Show example

```
storage::*> storage port show -port-type ENET
```

		Speed				
VLAN	Node	Port	Type	Mode	(Gb/s)	State
ID						Status
-----						
----						
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
```

### Show example

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

```
There are no entries matching your query.
```

## Step 2: Copy the RCF to Cisco switch S2

1. 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](#).

### Show example

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#
```

2. Apply the RCF previously downloaded to the bootflash:

```
copy bootflash:
```

### Show example

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
```

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.



In the banner output from the `show banner motd` command, you must read and follow the instructions in the **IMPORTANT NOTES** section to make sure the proper configuration and operation of the switch.

## Show example

```
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.

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 S2.

For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 3000 Series NX-OS Command References](#).

#### Show example

The following example shows the `running-config` file successfully copied to the `startup-config` file:

```
S2# copy running-config startup-config
[#####] 100% Copy complete.
```

### Step 3: Copy the NX-OS image to Cisco switch S2 and reboot

1. Copy the NX-OS image to switch S2.

## Show example

```
S2# 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.
```

2. 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:

## Show example

```
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#
```

### 3. 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.

#### Show example

```
S2# copy running-config startup-config
[] 100% Copy complete.
S2# reload
This command will reboot the system. (y/n)? [n] y
```

### 4. Confirm that the new NX-OS version number is on the switch:

## Show example

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#
```

#### **Step 4: Recheck the health status of switches and ports**

1. Recheck that the storage switches are available after the reboot:

```
system switch ethernet show
```

## Show example

```
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::*>
```

2. Verify that the switch ports are healthy and operational after the reboot:

```
storage port show -port-type ENET
```

### Show example

```
storage::*> storage port show -port-type ENET
```

VLAN		Speed				
Node	Port	Type	Mode	(Gb/s)	State	Status
ID						
-----						
----						
node1						
30	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
node2						
30	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						

3. Recheck that there are no storage switch or cabling issues with the cluster:

```
system health alert show -instance
```

### Show example

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

There are no entries matching your query.

4. Repeat the procedure to upgrade the NX-OS software and RCF on switch S1.
5. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

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



## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.