End-of-availability switches

Cluster and storage switches

NetApp
May 08, 2024

Table of Contents

End-of-availability switches

End-of-availability

The following switches are no longer available for purchase, but are still supported.

- Cisco Nexus 3232C
- Cisco Nexus 3132Q-V
- Cisco Nexus 92300YC
- NetApp CN1610

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

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

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

Rail kit and cabinet documentation

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

Name	Description
42U System Cabinet, Deep Guide	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.
Install a Cisco Nexus 3232C switch in a NetApp Cabinet	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

Cluster switch A		Cluster switch B	
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
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

Cluster switch A		Cluster switch B	
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
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	

Cluster switch A		Cluster switch B	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 through 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 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 *Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet* guide for instructions to install the switch in a NetApp cabinet.
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 **yes**. The default is no.
Do you want to enforce secure password standard? (yes/no)	Respond with **yes**. The default is yes.
Enter the password for admin.	The default password is “admin”; you must create a new, strong password. A weak password can be rejected.
Would you like to enter the basic configuration dialog? (yes/no)	Respond with **yes** at the initial configuration of the switch.

Prompt	Response
Create another login account? (yes/no)	Your answer depends on your site's policies on alternate administrators. The default is **no**.
Configure read-only SNMP community string? (yes/no)	Respond with **no**. The default is no.
Configure read-write SNMP community string? (yes/no)	Respond with **no**. The default is no.
Enter the switch name.	The switch name is limited to 63 alphanumeric characters.
Continue with Out-of-band (mgmt0) management configuration? (yes/no)	Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip_address.
Configure the default-gateway? (yes/no)	Respond with **yes**. At the IPv4 address of the default-gateway: prompt, enter your default_gateway.
Configure advanced IP options? (yes/no)	Respond with **no**. The default is no.
Enable the telnet service? (yes/no)	Respond with **no**. The default is no.
Enabled SSH service? (yes/no)	Respond with **yes**. The default is yes. ⓘ SSH is recommended when using Cluster Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.
Enter the type of SSH key you want to generate (dsa/rsa/rsa1).	The default is **rsa**.
Enter the number of key bits (1024-2048).	Enter the number of key bits from 1024-2048.
Configure the NTP server? (yes/no)	Respond with **no**. The default is no.
Configure default interface layer (L3/L2):	Respond with **L2**. The default is L2.
Configure default switch port interface state (shut/noshut):	Respond with **noshut**. The default is noshut.

Prompt	Response
Configure CoPP system profile (strict/moderate/lenient/dense):	Respond with **strict**. The default is strict.
Would you like to edit the configuration? (yes/no)	You should see the new configuration at this point. Review and make any necessary changes to the configuration you just entered. Respond with **no** at the prompt if you are satisfied with the configuration. Respond with **yes** if you want to edit your configuration settings.
Use this configuration and save it? (yes/no)	Respond with **yes** to save the configuration. This automatically updates the kickstart and system images. ⓘ If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch.

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

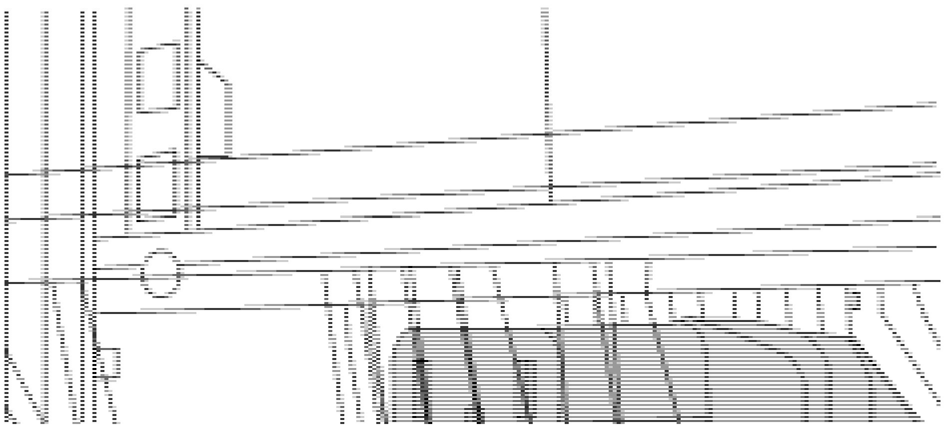
  a. Determine the vertical location of the switches and blanking panel in the cabinet.

     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.

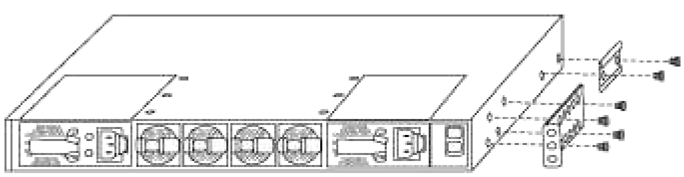
  d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



(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.

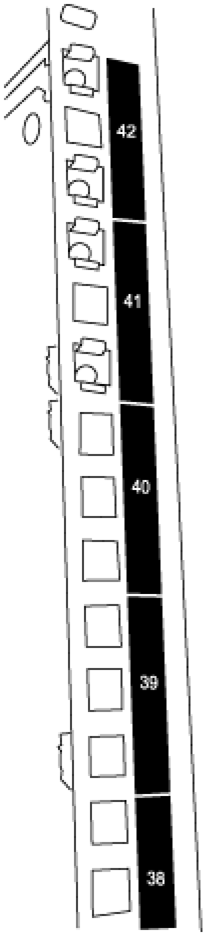
   

   b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.

   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.

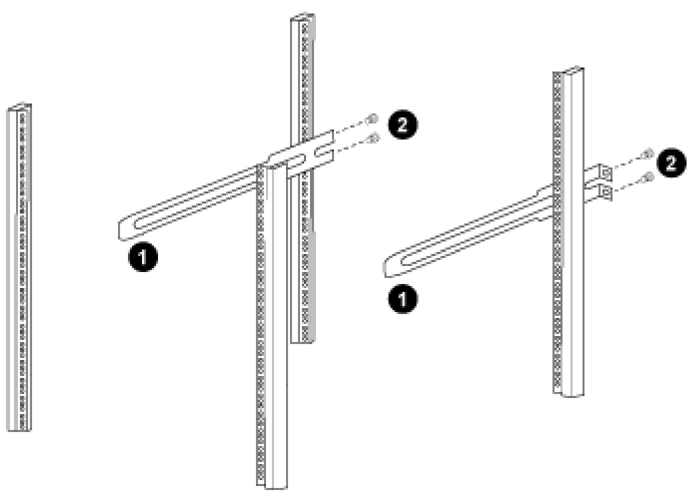
2. Install the clip nuts in the square hole locations for all four IEA posts.



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.

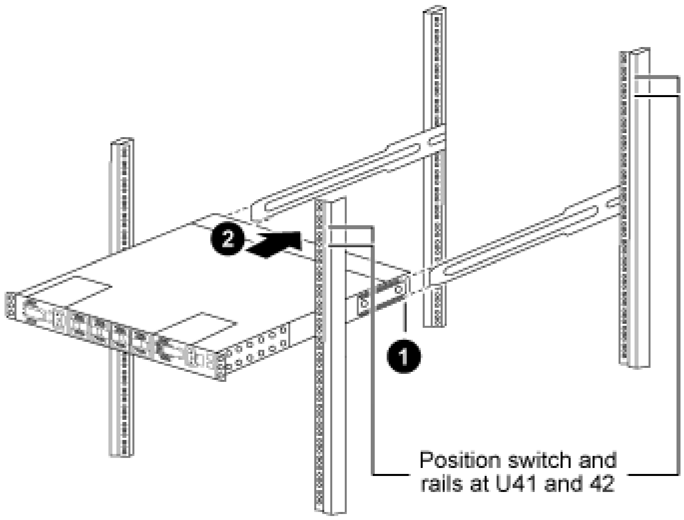
   b. Repeat step 4a for the right side rear post.

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.

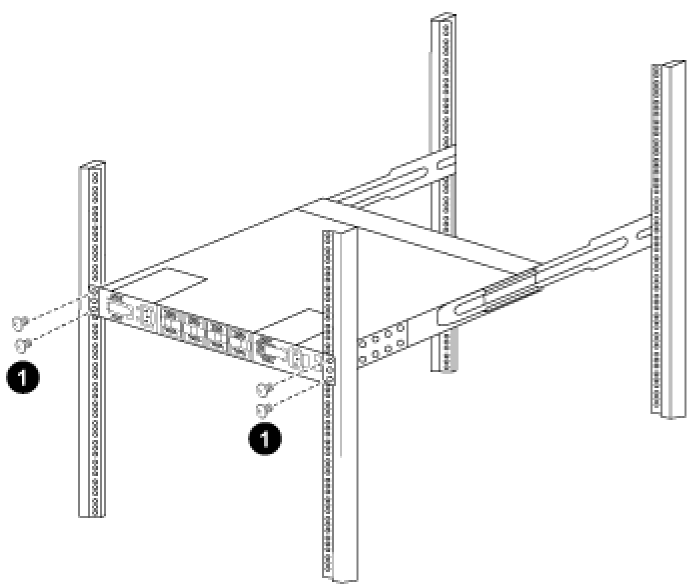
a. Position the back of the switch at RU41.



(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/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
             e0a    cs1                       Eth1/2            N3K-
C3232C
             e0b    cs2                       Eth1/2            N3K-
C3232C
cluster1-01/cdp
             e0a    cs1                       Eth1/1            N3K-
C3232C
             e0b    cs2                       Eth1/1            N3K-
C3232C

4 entries were displayed.
```

4. Check the administrative or operational status of each cluster interface.

   a. Display the network port attributes:

   `network port show –ipspace Cluster`

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

            Logical            Status     Network
Current       Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01   e0a     true
            cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01   e0b     true
            cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02   e0a     true
            cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02   e0b     true

4 entries were displayed.
```

5. Ping the remote cluster LIFs: `cluster ping-cluster -node` *`node-name`*

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

          Logical
Vserver   Interface           Auto-revert
--------- -------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
4 entries were displayed.
```

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

   `system switch ethernet log enable-collection`

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
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

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

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

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: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                             cluster-network     10.233.205.93
NX3232C
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

3. Disable auto-revert on the cluster LIFs.

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

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

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: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
```

```
N3K-C3232C
      Serial Number: FOXXXXXXXGS
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                     9.3(4)
     Version Source: CDP

2 entries were displayed.
```

> You might observe the following output on the cs1 switch console depending on the RCF version previously loaded on the switch
>
> ```
> 2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
> UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
> VLAN0092. Port consistency restored.
> 2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-
> BLOCK_PVID_PEER: Blocking port-channel1 on VLAN0001.
> Inconsistent peer vlan.
> 2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-
> BLOCK_PVID_LOCAL: Blocking port-channel1 on VLAN0092.
> Inconsistent local vlan.
> ```

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

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

24. 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) --
.
.
```

25. 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#
```

26. 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` *`vserver_name`* `-lif` *`lif_name`*

27. 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::*>
```

28. 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
RSA keys not present	Regenerate ONTAP SSH keys. Contact NetApp support.
switch password error	Verify credentials, test SSH connectivity, and regenerate ONTAP SSH keys. Review the switch documentation or contact NetApp support for instructions.
ECDSA keys not present for FIPS	If FIPS mode is enabled, ECDSA keys need to be generated on the switch before retrying.
pre-existing log found	Remove the previous log collection file on the switch.

switch dump log error	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: cshm1!
                                  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

       Local  Discovered
Node   Port   Device       Interface   Platform
------ ------ ------------ ----------- ----------
n1     /cdp
        e0a   CL1          0/1         CN1610
        e0b   CL2          0/1         CN1610
        e0c   CL2          0/2         CN1610
        e0d   CL1          0/2         CN1610
n2     /cdp
        e0a   CL1          0/3         CN1610
        e0b   CL2          0/3         CN1610
        e0c   CL2          0/4         CN1610
        e0d   CL1          0/4         CN1610

8 entries were displayed.
```

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

      `network port show -role cluster`

Show example

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

Node: n1
                Broadcast              Speed (Mbps) Health Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status Health
Status
----- --------- ---------- ----- ----- ------------ ------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -
e0b   cluster   cluster    up    9000  auto/10000     -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -
Node: n2
                Broadcast              Speed (Mbps) Health Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status Health
Status
----- --------- ---------- ----- ----- ------------ ------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -
e0b   cluster   cluster    up    9000  auto/10000     -
e0c   cluster   cluster    up    9000  auto/10000     -
e0d   cluster   cluster    up    9000  auto/10000     -

8 entries were displayed.
```

b. Display information about the logical interfaces:

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

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        e0b
true
         n1_clus3   up/up       10.10.0.3/24    n1        e0c
true
         n1_clus4   up/up       10.10.0.4/24    n1        e0d
true
         n2_clus1   up/up       10.10.0.5/24    n2        e0a
true
         n2_clus2   up/up       10.10.0.6/24    n2        e0b
true
         n2_clus3   up/up       10.10.0.7/24    n2        e0c
true
         n2_clus4   up/up       10.10.0.8/24    n2        e0d
true

 8 entries were displayed.
```

c. Display information about the discovered cluster switches:

`system cluster-switch show`

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
Model
------------------------------ ---------------- -------------
--------
CL1                                cluster-network  10.10.1.101
CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP
CL2                                cluster-network  10.10.1.102
CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

2   entries displayed.
```

4. Verify that the appropriate RCF and image are installed on the new 3232C switches as necessary for your requirements, and make any essential site customizations.

   You should prepare both switches at this time. If you need to upgrade the RCF and image, you must complete the following procedure:

   a. See the Cisco Ethernet Switch page on the NetApp Support Site.

   b. Note your switch and the required software versions in the table on that page.

   c. Download the appropriate version of the RCF.

   d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.

   e. Download the appropriate version of the image software at Cisco® Cluster and Management Network Switch Reference Configuration File Download.

5. Migrate the LIFs associated with the second CN1610 switch that you plan to replace:

   `network interface migrate -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
Home
-------- ---------- ----------- --------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24    n1        e0a
true
         n1_clus2   up/up       10.10.0.2/24    n1        e0a
false
         n1_clus3   up/up       10.10.0.3/24    n1        e0d
false
         n1_clus4   up/up       10.10.0.4/24    n1        e0d
true
         n2_clus1   up/up       10.10.0.5/24    n2        e0a
true
         n2_clus2   up/up       10.10.0.6/24    n2        e0a
false
         n2_clus3   up/up       10.10.0.7/24    n2        e0d
false
         n2_clus4   up/up       10.10.0.8/24    n2        e0d
true

8 entries were displayed.
```

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

8 entries were displayed.
```

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

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

8 entries were displayed.
```

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
         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.
```

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     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)
```

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

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

8 entries were displayed.
```

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

8 entries were displayed.
```

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

       Local  Discovered
Node   Port   Device       Interface       Platform
------ ------ ------------ --------------- -------------
n1     /cdp
        e0a   C1           Ethernet1/1/1   N3K-C3232C
        e0b   C2           Ethernet1/1/1   N3K-C3232C
        e0c   C2           Ethernet1/1/2   N3K-C3232C
        e0d   C1           Ethernet1/1/2   N3K-C3232C
n2     /cdp
        e0a   C1           Ethernet1/1/3   N3K-C3232C
        e0b   C2           Ethernet1/1/3   N3K-C3232C
        e0c   C2           Ethernet1/1/4   N3K-C3232C
        e0d   C1           Ethernet1/1/4   N3K-C3232C

n3     /cdp
        e4a   C1           Ethernet1/7     N3K-C3232C
        e4e   C2           Ethernet1/7     N3K-C3232C

n4     /cdp
        e4a   C1           Ethernet1/8     N3K-C3232C
        e4e   C2           Ethernet1/8     N3K-C3232C

12 entries were displayed.
cluster::*> network port show -role cluster
(network port show)

Node: n1
                Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -
e0b   cluster   cluster    up    9000  auto/10000     -
e0c   cluster   cluster    up    9000  auto/10000     -         -
e0d   cluster   cluster    up    9000  auto/10000     -         -
```

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

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

Node: n4
                Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e4a   cluster   cluster    up    9000  auto/40000     -
e4e   cluster   cluster    up    9000  auto/40000     -

12 entries were displayed.

cluster::*> network interface show -role cluster
(network interface show)
         Logical    Status      Network        Current  Current
Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
```

```
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true
         n3_clus1   up/up       10.10.0.9/24   n3       e4a
true
         n3_clus2   up/up       10.10.0.10/24  n3       e4e
true
         n4_clus1   up/up       10.10.0.11/24  n4       e4a
true
         n4_clus2   up/up       10.10.0.12/24  n4       e4e
true

12 entries were displayed.

cluster::> system cluster-switch show

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

     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I6(1)
    Version Source: CDP

C2                          cluster-network  10.10.1.104
NX3232C

     Serial Number: FOX000002
      Is Monitored: true
            Reason:
```

```
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I6(1)
    Version Source: CDP
CL1                         cluster-network  10.10.1.101   CN1610

     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP
CL2                         cluster-network  10.10.1.102
CN1610

     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP 4 entries were displayed.
```

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                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3232C

     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I6(1)
    Version Source: CDP

C2                          cluster-network    10.10.1.104
NX3232C
     Serial Number: FOX000002
      Is Monitored: true
          Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I6(1)
    Version Source: CDP

2 entries were displayed.
```

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
            Local  Discovered
Node        Port   Device              Interface        Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e0a    CL1                 Ethernet1/1      N5K-C5596UP
            e0b    CL2                 Ethernet1/1      N5K-C5596UP
            e0c    CL2                 Ethernet1/2      N5K-C5596UP
            e0d    CL1                 Ethernet1/2      N5K-C5596UP
n2         /cdp
            e0a    CL1                 Ethernet1/3      N5K-C5596UP
            e0b    CL2                 Ethernet1/3      N5K-C5596UP
            e0c    CL2                 Ethernet1/4      N5K-C5596UP
            e0d    CL1                 Ethernet1/4      N5K-C5596UP
8 entries were displayed.
```

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

      `network port show -role cluster`

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

Node: n2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

b. Display information about the logical interfaces:

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

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

c. Display information about the discovered cluster switches:

```
system cluster-switch show
```

Show example

The following example shows the active cluster switches:

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

Switch                        Type               Address
Model
----------------------------- ------------------ ---------------
---------------
CL1                           cluster-network    10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP
CL2                           cluster-network    10.10.1.102
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP

2 entries were displayed.
```

4. Verify that the appropriate RCF and image are installed on the new 3232C switches as necessary for your requirements, and make the essential site customizations, such as users and passwords, network addresses, and other customizations.

   ⓘ You must prepare both switches at this time.

   If you need to upgrade the RCF and image, you must complete the following steps:

   a. Go to the *Cisco Ethernet Switches* page on the NetApp Support Site.

      Cisco Ethernet Switches

   b. Note your switch and the required software versions in the table on that page.
   c. Download the appropriate version of the RCF.
   d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the

instructions on the **Download** page to download the RCF.

e. Download the appropriate version of the image software.

   See the *ONTAP 8.x or later Cluster and Management Network Switch Reference Configuration Files* Download page, and then click the appropriate version.

   To find the correct version, see the *ONTAP 8.x or later Cluster Network Switch Download page*.

5. Migrate the LIFs associated with the second Nexus 5596 switch to be replaced:

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

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

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` *`vserver-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

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

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

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
                                                  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.
```

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

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
            Local  Discovered
Node        Port   Device              Interface        Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e0a    C1                 Ethernet1/1/1    N3K-C3232C
            e0b    C2                 Ethernet1/1/1    N3K-C3232C
            e0c    C2                 Ethernet1/1/2    N3K-C3232C
            e0d    C1                 Ethernet1/1/2    N3K-C3232C
n2         /cdp
            e0a    C1                 Ethernet1/1/3    N3K-C3232C
            e0b    C2                 Ethernet1/1/3    N3K-C3232C
            e0c    C2                 Ethernet1/1/4    N3K-C3232C
            e0d    C1                 Ethernet1/1/4    N3K-C3232C
n3         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3232C
            e4e    C2                 Ethernet1/7      N3K-C3232C
n4         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3232C
            e4e    C2                 Ethernet1/8      N3K-C3232C
12 entries were displayed.
```

+

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

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

```
-

Node: n2

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

Node: n3

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

Node: n4

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

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

+

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

+

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

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3232C
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.104
NX3232C
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

CL1                           cluster-network   10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP
CL2                           cluster-network    10.10.1.102
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.1(1)N1(1)
    Version Source: CDP

4 entries were displayed.
```

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                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3232C
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.104
NX3232C
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

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 supportedQSFP/ QSFP28 optical modules with fiber cables or QSFP/QSFP28 copper direct-attach cables.
  - The cluster switches require the appropriate ISL cabling: 2x QSFP28 fiber or copper direct-attach cables.
- 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
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
Node: n2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- -----
e4a       Cluster      Cluster          up   9000 auto/40000  -
e4e       Cluster      Cluster          up   9000 auto/40000  -
4 entries were displayed.
```

b. Display information about the logical interfaces and their designated home nodes:

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

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.
```

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

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
            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.
```

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                          Type                 Address
Model
--------------------------- ------------------ ----------------
---------------
C1                              cluster-network     10.10.1.101
NX3232CV
Serial Number: FOX000001
Is Monitored: true
Reason:
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version 7.0(3)I6(1)
Version Source: CDP

C2                              cluster-network      10.10.1.102
NX3232CV
Serial Number: FOX000002
Is Monitored: true
Reason:
Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version 7.0(3)I6(1)
Version Source: CDP 2 entries were displayed.
```

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
             Local  Discovered
Node         Port   Device              Interface         Platform
----------- ------ ------------------- ----------------
----------------
n1          /cdp
             e0a    CL1                 Ethernet1/1/1    N3K-C3232C
             e0b    CL2                 Ethernet1/1/1    N3K-C3232C
             e0c    CL2                 Ethernet1/1/2    N3K-C3232C
             e0d    CL1                 Ethernet1/1/2    N3K-C3232C

n2          /cdp
             e0a    CL1                 Ethernet1/1/3    N3K-C3232C
             e0b    CL2                 Ethernet1/1/3    N3K-C3232C
             e0c    CL2                 Ethernet1/1/4    N3K-C3232C
             e0d    CL1                 Ethernet1/1/4    N3K-C3232C

n3          /cdp
             e4a    CL1                 Ethernet1/7      N3K-C3232C
             e4e    CL2                 Ethernet1/7      N3K-C3232C

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

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
                                                  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  -
```

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

   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 *vserver-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
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
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  -

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                      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

C2                          cluster-network    10.10.1.103
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. 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
                                      Speed                       VLAN
Node               Port Type  Mode    (Gb/s) State    Status        ID
------------------ ---- ----- ------- ------ -------- --------- ----
node1
                   e3a  ENET  storage    100 enabled  online        30
                   e3b  ENET  storage      0 enabled  offline       30
                   e7a  ENET  storage      0 enabled  offline       30
                   e7b  ENET  storage      0 enabled  offline       30
node2
                   e3a  ENET  storage    100 enabled  online        30
                   e3b  ENET  storage      0 enabled  offline       30
                   e7a  ENET  storage      0 enabled  offline       30
                   e7b  ENET  storage      0 enabled  offline       30
```

3. Verify that storage switch S1 is available:

```
network device-discovery show
```

Show example

```
storage::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
----------------
node1/cdp
            e3a    S1                        Ethernet1/1
NX3232C
            e4a    node2                     e4a              AFF-
A700
            e4e    node2                     e4e              AFF-
A700
node1/lldp
            e3a    S1                        Ethernet1/1      -
            e4a    node2                     e4a              -
            e4e    node2                     e4e              -
node2/cdp
            e3a    S1                        Ethernet1/2
NX3232C
            e4a    node1                     e4a              AFF-
A700
            e4e    node1                     e4e              AFF-
A700
node2/lldp
            e3a    S1                        Ethernet1/2      -
            e4a    node1                     e4a              -
            e4e    node1                     e4e              -
```

4. Run the `show lldp neighbors` command on the working switch to confirm that you can see both nodes and all shelves:

```
show lldp neighbors
```

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
                                      Speed
VLAN
Node                   Port Type  Mode    (Gb/s) State    Status
ID
------------------ ---- ----- ------- ------ -------- ------------
---
node1
                   e3a  ENET  storage    100 enabled  online
30
                   e3b  ENET  storage      0 enabled  offline
30
                   e7a  ENET  storage      0 enabled  offline
30
                   e7b  ENET  storage    100 enabled  online
30
node2
                   e3a  ENET  storage    100 enabled  online
30
                   e3b  ENET  storage      0 enabled  offline
30
                   e7a  ENET  storage      0 enabled  offline
30
                   e7b  ENET  storage    100 enabled  online
30
```

2. Verify that both switches are available:

```
network device-discovery show
```

Show example

```
storage::*> network device-discovery show
Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
node1/cdp
             e3a    S1                        Ethernet1/1
NX3232C
             e4a    node2                     e4a              AFF-
A700
             e4e    node2                     e4e              AFF-
A700
             e7b    NS2                       Ethernet1/1
NX3232C
node1/lldp
             e3a    S1                        Ethernet1/1      -
             e4a    node2                     e4a              -
             e4e    node2                     e4e              -
             e7b    NS2                       Ethernet1/1      -
node2/cdp
             e3a    S1                        Ethernet1/2
NX3232C
             e4a    node1                     e4a              AFF-
A700
             e4e    node1                     e4e              AFF-
A700
             e7b    NS2                       Ethernet1/2
NX3232C
node2/lldp
             e3a    S1                        Ethernet1/2      -
             e4a    node1                     e4a              -
             e4e    node1                     e4e              -
             e7b    NS2                       Ethernet1/2      -
```

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.

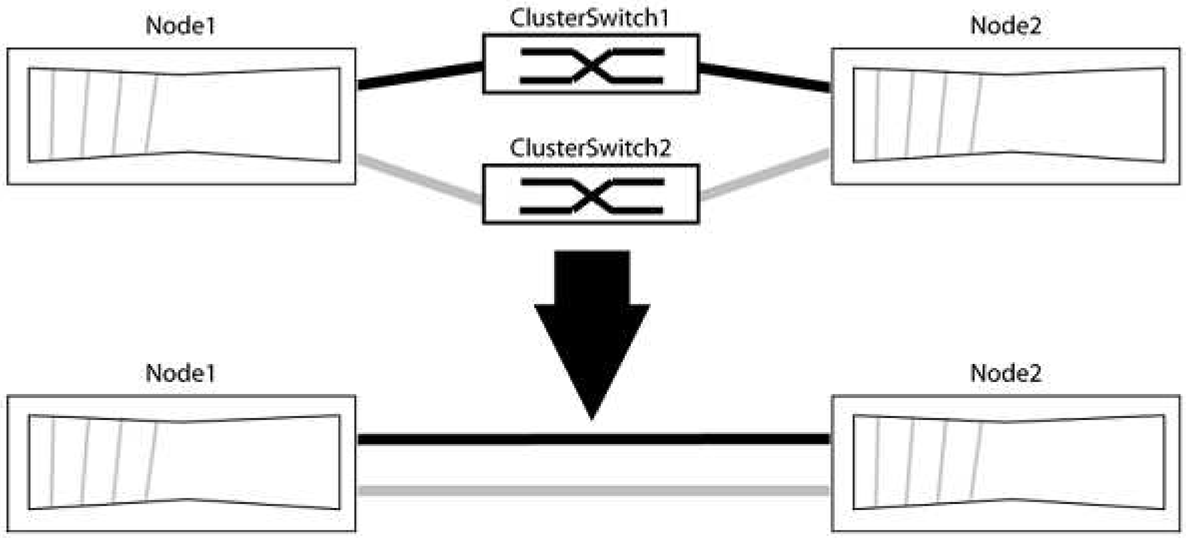
What you'll need

- 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

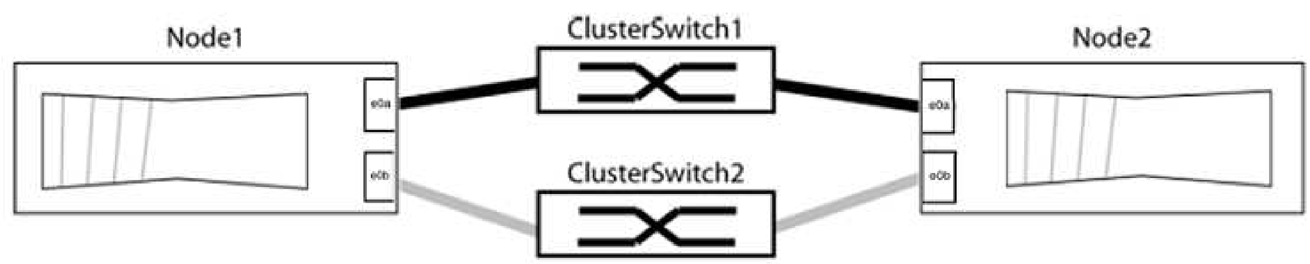
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

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
   ```

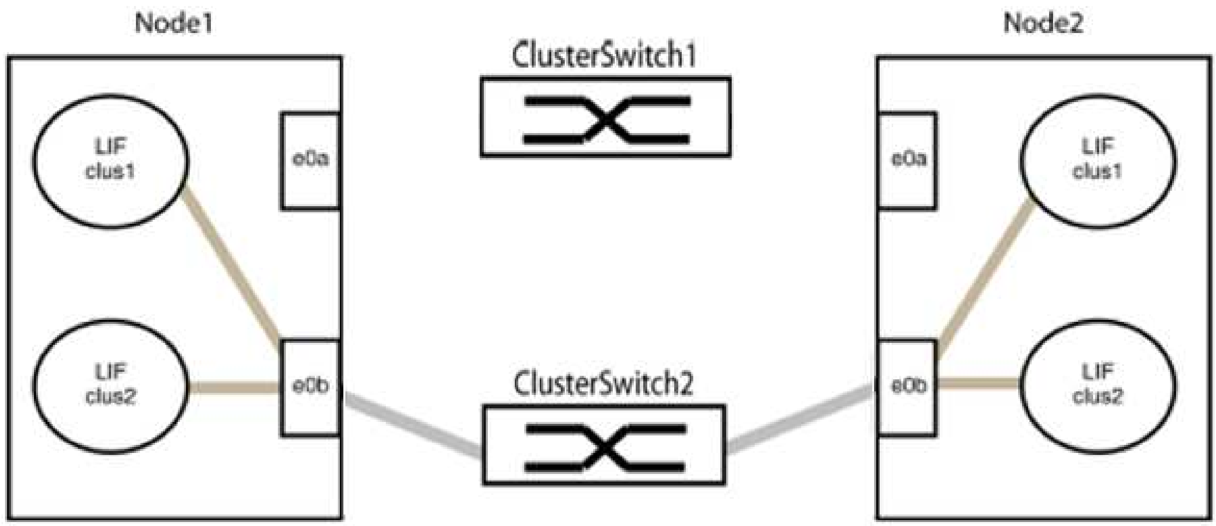
   All units must be either master or secondary.

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**.

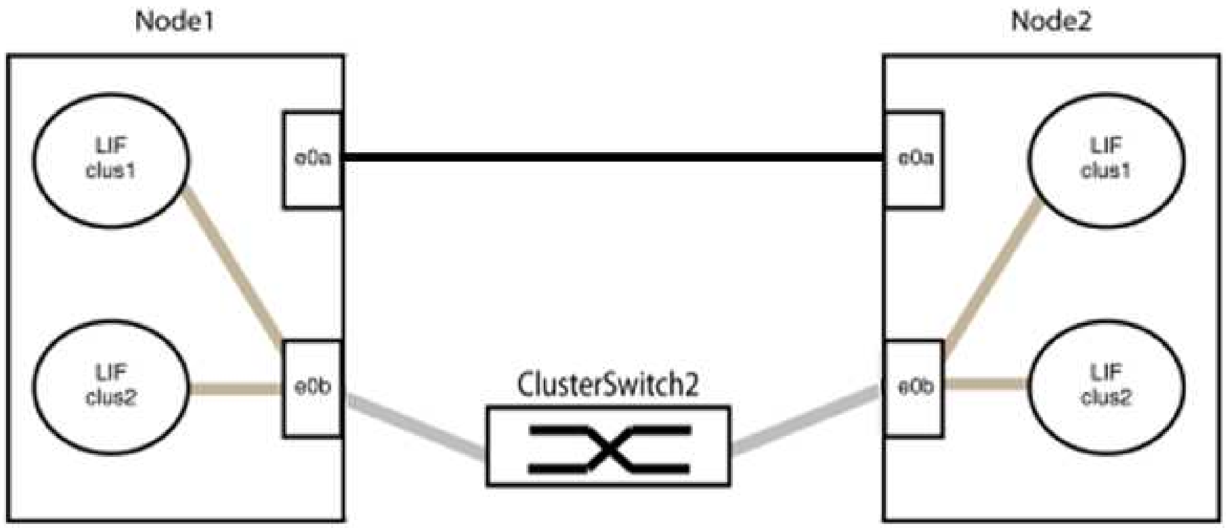
   a. Disconnect all the cables from the ports in group1 at the same time.

      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:



9. The switchless cluster network option transitions from `false` to `true`. This might take up to 45 seconds. Confirm that the switchless option is set to `true`:

   `network options switchless-cluster show`

   The following example shows that the switchless cluster is enabled:

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

10. Verify that the cluster network is not disrupted:

    `cluster ping-cluster -node local`

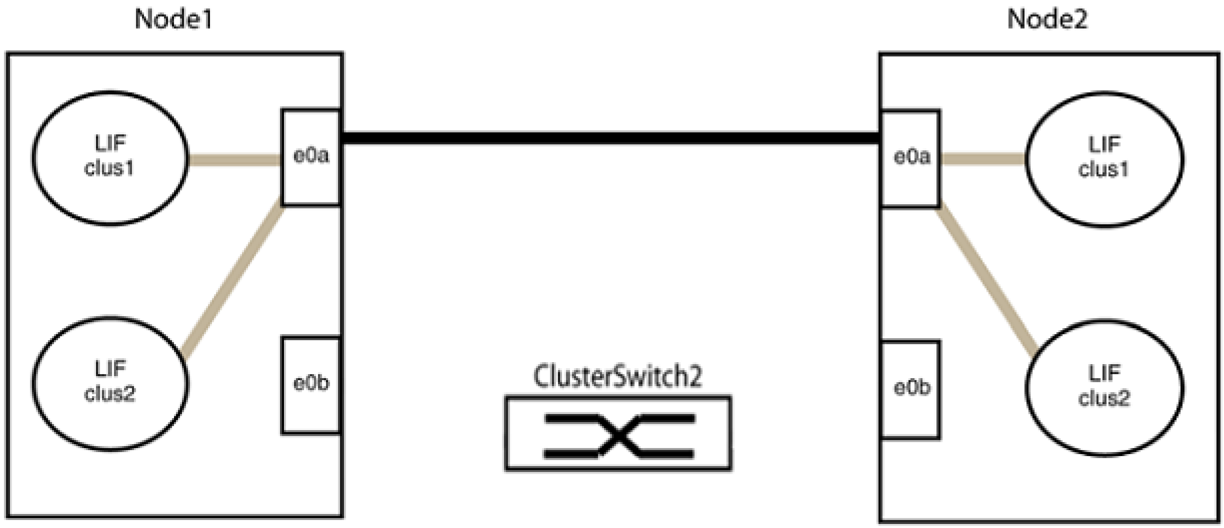
    > Before proceeding to the next step, you must wait at least two minutes to confirm a working back-to-back connection on group 1.

11. Set up the switchless configuration for the ports in group 2.

    > To avoid potential networking issues, you must disconnect the ports from group2 and reconnect them back-to-back as quickly as possible, for example, **in less than 20 seconds**.

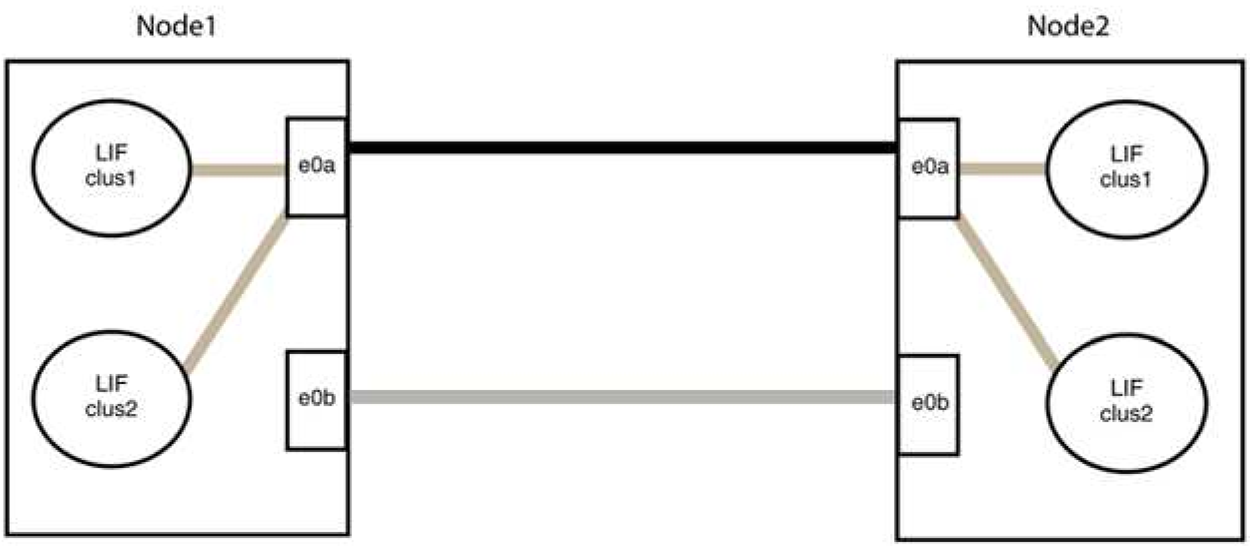
    a. Disconnect all the cables from the ports in group2 at the same time.

       In the following example, the cables are disconnected from port "e0b" on each node, and cluster traffic continues through the direct connection between the "e0a" ports:



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

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



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, 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    Status
ID
------------------ ---- ----- ------- ------ -------- -----------
----
node1
                   e3a  ENET  storage    100 enabled  online
30
                   e3b  ENET  storage      0 enabled  offline
30
                   e7a  ENET  storage      0 enabled  offline
30
                   e7b  ENET  storage    100 enabled  online
30
node2
                   e3a  ENET  storage    100 enabled  online
30
                   e3b  ENET  storage      0 enabled  offline
30
                   e7a  ENET  storage      0 enabled  offline
30
                   e7b  ENET  storage    100 enabled  online
30
```

4. Check that there are no storage switch or cabling issues:

`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
                                      Speed
VLAN
Node                   Port Type  Mode    (Gb/s) State    Status
ID
------------------ ---- ----- ------- ------ -------- -----------
----
node1
                       e3a  ENET  storage    100 enabled  online
30
                       e3b  ENET  storage      0 enabled  offline
30
                       e7a  ENET  storage      0 enabled  offline
30
                       e7b  ENET  storage    100 enabled  online
30
node2
                       e3a  ENET  storage    100 enabled  online
30
                       e3b  ENET  storage      0 enabled  offline
30
                       e7a  ENET  storage      0 enabled  offline
30
                       e7b  ENET  storage    100 enabled  online
30
```

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`

Cisco Nexus 3132Q-V

Overview

Overview of installation and configuration for Cisco Nexus 3132Q-V switches

Cisco Nexus 3132Q-V 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 3132Q-V switch on systems running ONTAP, follow these steps:

1. Complete Cisco Nexus 3132Q-V 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 3132Q-V cluster switch in a NetApp cabinet. install the Cisco Nexus 3132Q-V switch and pass-through panel in a NetApp cabinet with the standard brackets that are included with the switch.
3. Configure the Cisco Nexus 3132Q-V switch. Set up and configure the Cisco Nexus 3132Q-V 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. Follow this procedure to install the NX-OS software on the Nexus 3132Q-V cluster switch.
6. Install the Reference Configuration File (RCF). Follow this procedure to install the RCF after setting up the Nexus 3132Q-V switch for the first time. You can also use this procedure to upgrade your RCF version.

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 3132Q-V switches

For Cisco Nexus 3132Q-V switch installation and maintenance, be sure to review network and configuration 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 3132Q-V switches

For Cisco Nexus 3132Q-V switch installation and maintenance, be sure to review all the recommended documentation.

Switch documentation

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

Document title	Description
Nexus 3000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 3000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 3000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 3000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 3000 switches.
Nexus 3000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 3000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 3000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 3000 Series.

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

Rail kit and cabinet documentation

To install a 3132Q-V Cisco switch in a NetApp cabinet, see the following hardware documentation.

Name	Description
42U System Cabinet, Deep Guide	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.
Install Cisco Nexus 3132Q-V switch in a NetApp Cabinet	Describes how to install a Cisco Nexus 3132Q-V 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 3132Q-V 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 40GbE port or 4 x 10GbE ports.

Sample cabling worksheet

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

Cluster switch A		**Cluster switch B**	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x10G/40G node	1	4x10G/40G node
2	4x10G/40G node	2	4x10G/40G node
3	4x10G/40G node	3	4x10G/40G node
4	4x10G/40G node	4	4x10G/40G node
5	4x10G/40G node	5	4x10G/40G node
6	4x10G/40G node	6	4x10G/40G node
7	4x10G/40G node	7	4x10G/40G node
8	4x10G/40G node	8	4x10G/40G node
9	4x10G/40G node	9	4x10G/40G node
10	4x10G/40G node	10	4x10G/40G node
11	4x10G/40G node	11	4x10G/40G node
12	4x10G/40G node	12	4x10G/40G node

Cluster switch A		Cluster switch B	
13	4x10G/40G node	13	4x10G/40G node
14	4x10G/40G node	14	4x10G/40G node
15	4x10G/40G node	15	4x10G/40G node
16	4x10G/40G node	16	4x10G/40G node
17	4x10G/40G node	17	4x10G/40G node
18	4x10G/40G node	18	4x10G/40G node
19	40G node 19	19	40G node 19
20	40G node 20	20	40G node 20
21	40G node 21	21	40G node 21
22	40G node 22	22	40G node 22
23	40G node 23	23	40G node 23
24	40G node 24	24	40G node 24
25 through 30	Reserved	25 through 30	Reserved
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32

Blank cabling worksheet

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

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

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

Cluster switch A		Cluster switch B	
25 through 30	Reserved	25 through 30	Reserved
31	40G ISL to switch B port 31	31	40G ISL to switch A port 31
32	40G ISL to switch B port 32	32	40G ISL to switch A port 32

Configure the Cisco Nexus 3132Q-V switch

Follow this procedure to configure the Cisco Nexus 3132Q-V 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 network switch documentation, controller documentation, and ONTAP documentation. For more information, see Required documentation.
- Applicable licenses, network and configuration information, and cables.
- Completed cabling worksheets. See Complete Cisco Nexus 3132Q-V cabling worksheet.
- Applicable NetApp cluster network and management network RCFs, downloaded from the NetApp Support Site at 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 3132Q-V in a NetApp system cabinet	See the *Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet* guide for instructions to install the switch in a NetApp cabinet.
Equipment in a Telco rack	See the procedures provided in the switch hardware installation guides and the NetApp installation and setup instructions.

2. Cable the cluster network and management network switches to the controllers using the completed cabling worksheet, as described in Complete Cisco Nexus 3132Q-V cabling worksheet.
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 **yes**. The default is no.
Do you want to enforce secure password standard? (yes/no)	Respond with **yes**. The default is yes.
Enter the password for admin:	The default password is “admin”; you must create a new, strong password. A weak password can be rejected.
Would you like to enter the basic configuration dialog? (yes/no)	Respond with **yes** at the initial configuration of the switch.
Create another login account? (yes/no)	Your answer depends on your site’s policies on alternate administrators. The default is **no**.
Configure read-only SNMP community string? (yes/no)	Respond with **no**. The default is no.
Configure read-write SNMP community string? (yes/no)	Respond with **no**. The default is no.
Enter the switch name.	The switch name is limited to 63 alphanumeric characters.
Continue with Out-of-band (mgmt0) management configuration? (yes/no)	Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip_address.
Configure the default-gateway? (yes/no)	Respond with **yes**. At the IPv4 address of the default-gateway: prompt, enter your default_gateway.
Configure advanced IP options? (yes/no)	Respond with **no**. The default is no.
Enable the telnet service? (yes/no)	Respond with **no**. The default is no.
Enabled SSH service? (yes/no)	Respond with **yes**. The default is yes. SSH is recommended when using Cluster Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.
Enter the type of SSH key you want to generate (dsa/rsa/rsa1).	The default is **rsa**.

Prompt	Response
Enter the number of key bits (1024-2048).	Enter the key bits from 1024-2048.
Configure the NTP server? (yes/no)	Respond with **no**. The default is no.
Configure default interface layer (L3/L2):	Respond with **L2**. The default is L2.
Configure default switch port interface state (shut/noshut):	Respond with **noshut**. The default is noshut.
Configure CoPP system profile (strict/moderate/lenient/dense):	Respond with **strict**. The default is strict.
Would you like to edit the configuration? (yes/no)	You should see the new configuration at this point. Review and make any necessary changes to the configuration you just entered. Respond with **no** at the prompt if you are satisfied with the configuration. Respond with **yes** if you want to edit your configuration settings.
Use this configuration and save it? (yes/no)	Respond with **yes** to save the configuration. This automatically updates the kickstart and system images. ⓘ If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch.

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 3132Q-V cluster switch in a NetApp cabinet

Depending on your configuration, you might need to install the Cisco Nexus 3132Q-V switch and pass-through panel in a NetApp cabinet with the standard brackets that are included with the switch.

What you'll need

- The initial preparation requirements, kit contents, and safety precautions in the Cisco Nexus 3000 Series Hardware Installation Guide. Review these documents before you begin the procedure.
- The pass-through panel kit, 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

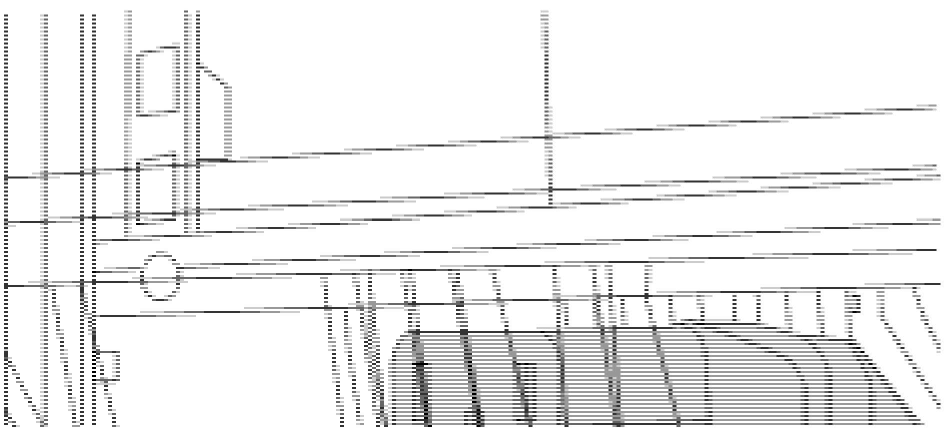
- Eight 10-32 or 12-24 screws and clip nuts to mount the brackets and slider rails to the front and rear cabinet posts.
- Cisco standard rail kit to install the switch in a NetApp cabinet.

> 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

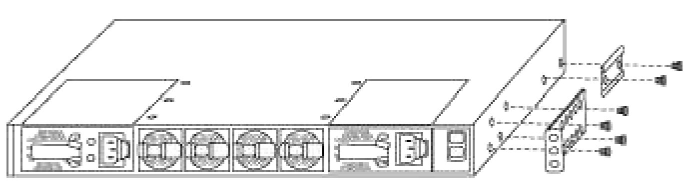
1. Install the pass-through blanking panel in the NetApp cabinet.
   a. Determine the vertical location of the switches and blanking panel in the cabinet.

      In this procedure, the blanking panel will be installed in U40.
   b. Install two clip nuts on each side in the appropriate square holes for front cabinet rails.
   c. Center the panel vertically to prevent intrusion into adjacent rack space, and then tighten the screws.
   d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



(1) Female connector of the jumper cord.

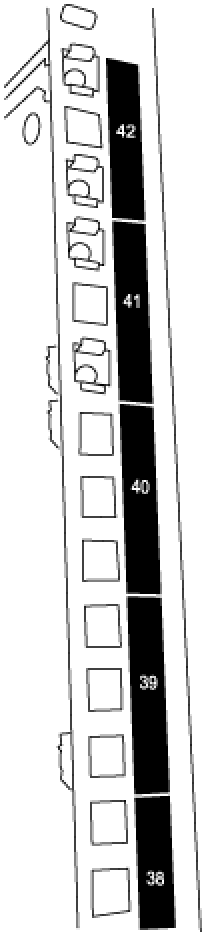
2. Install the rack-mount brackets on the Nexus 3132Q-V switch chassis.
   a. Position a front rack-mount bracket on one side of the switch chassis so that the mounting ear is aligned with the chassis faceplate (on the PSU or fan side), and then use four M4 screws to attach the bracket to the chassis.



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

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

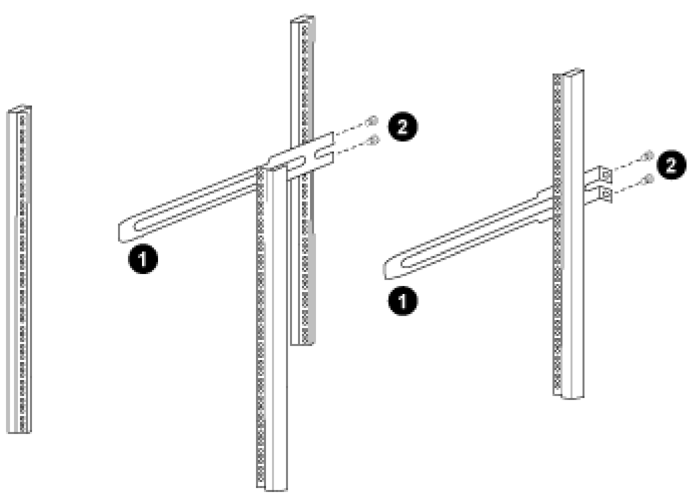
3. Install the clip nuts in the square hole locations for all four IEA posts.



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

4. Install the slider rails in the cabinet.

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



(1) As you gently slide the slider rail, align it to the screw holes in the rack.

(2) Tighten the screws of the slider rails to the cabinet posts.

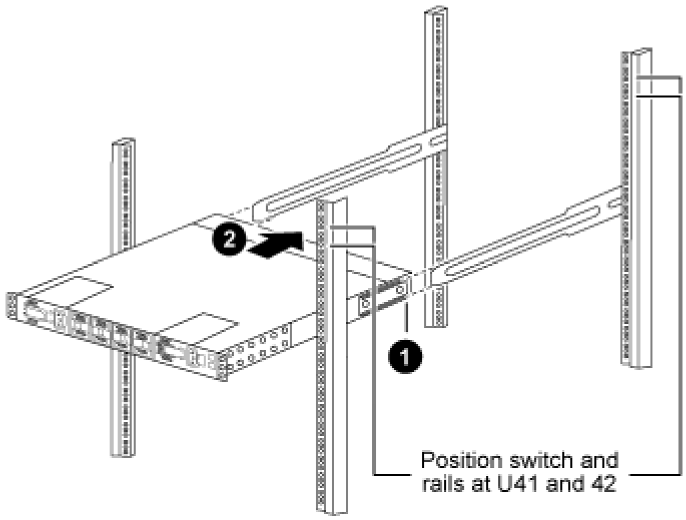
b. Repeat step 4a for the right side rear post.

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

5. Install the switch in the cabinet.

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

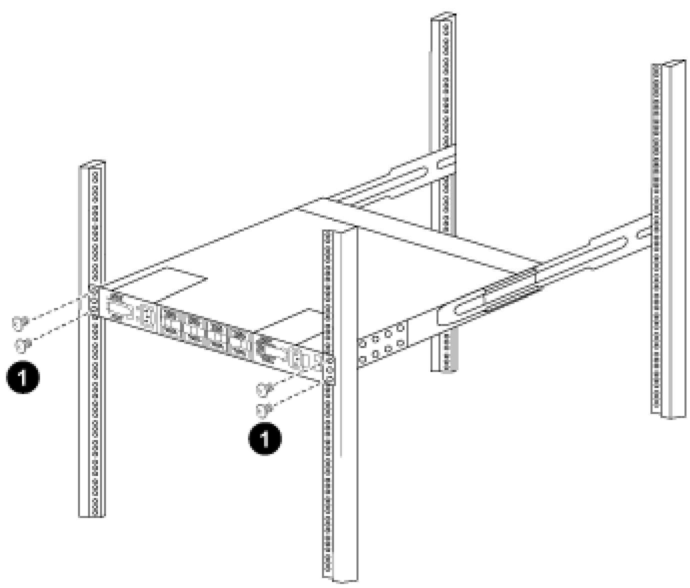
a. Position the back of the switch at RU41.



(1) As the chassis is pushed toward the rear posts, align the two rear rack-mount guides with the slider rails.

(2) Gently slide the switch until the front rack-mount brackets are flush with the front posts.

b. Attach the switch to the cabinet.



(1) With one person holding the front of the chassis level, the other person should fully tighten the four rear screws to the cabinet posts.

c. With the chassis now supported without assistance, fully tighten the front screws to the posts.

d. Repeat steps 5a through 5c for the second switch at the RU42 location.

> ⓘ By using the fully installed switch as a support, you do not need to hold the front of the second switch during the installation process.

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

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

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

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

Review cabling and configuration considerations

Before configuring your Cisco 3132Q-V 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

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.

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=xh
   ```

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

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

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

   ```
   set -privilege advanced
   ```

   The advanced prompt (`*>`) appears.

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

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

Show example

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

Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
             e0a    cs1                       Eth1/2            N3K-
C3132Q-V
             e0b    cs2                       Eth1/2            N3K-
C3132Q-V
cluster1-01/cdp
             e0a    cs1                       Eth1/1            N3K-
C3132Q-V
             e0b    cs2                       Eth1/1            N3K-
C3132Q-V
```

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

      `network port show –ipspace Cluster`

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
```

b. Display information about the LIFs:

`network interface show -vserver Cluster`

Show example

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

            Logical            Status     Network
Current       Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01   e0a     true
            cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01   e0b     true
            cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02   e0a     true
            cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02   e0b     true
```

5. Ping the remote cluster LIFs:

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

Show example

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

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

```
network interface show -vserver Cluster -fields auto-revert
```

Show example

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

          Logical
Vserver   Interface           Auto-revert
--------- ------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
```

What's next?

Install NX-OS software.

Install the NX-OS software

Follow this procedure to install the NX-OS software on the Nexus 3132Q-V 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).

Suggested documentation

- Cisco Ethernet switch. Consult the switch compatibility table for the supported ONTAP and NX-OS versions.
- Cisco Nexus 3000 Series Switches. Consult 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

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.

Be sure to complete the procedure in Prepare to install NX-OS software and Reference Configuration File, 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

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

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

3. Copy the NX-OS software to the Nexus 3132Q-V switch using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in Cisco Nexus 3000 Series NX-OS Command Reference guides.

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: xxxxxxxx
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

```
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 04.25
NXOS: version 9.3(3)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.3.bin
                  NXOS compile time: 12/22/2019 2:00:00 [12/22/2019
14:00:37]

Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash:   15137792 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
cs2#
```

5. Install the NX-OS image.

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

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        v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(01/28/2020)   no


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

```
Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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


Finishing the upgrade, switch will reboot in 10 seconds.
cs2#
```

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

```
show version
```

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 04.25
NXOS: version 9.3(4)
  BIOS compile time:  05/22/2019
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 06:28:31]



Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash:   15137792 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

What's next?

Install the Reference Configuration File (RCF).

Install the Reference Configuration File (RCF)

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

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. 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. Consult 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 software and Reference Configuration File, and then follow the steps below.

Step 1: Check port status

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-
C3132Q-V
             e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster1-02/cdp
             e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
             e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster1-03/cdp
             e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
             e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
             e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
             e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V
cluster1::*>
```

2. Check the administrative and operational status of each cluster port.

   a. Verify that all the cluster ports are up with a healthy status:

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

Show example

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

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

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

Show example

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
cluster1::*>
```

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

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

Show example

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                          Type                Address
Model
--------------------------- ------------------ ----------------
---------------
cs1                             cluster-network    10.0.0.1
NX3132QV
      Serial Number: FOXXXXXXXGS
       Is Monitored: true
             Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
     Version Source: CDP

cs2                             cluster-network    10.0.0.2
NX3132QV
      Serial Number: FOXXXXXXXGD
       Is Monitored: true
             Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
     Version Source: CDP

2 entries were displayed.
```

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

3. Disable auto-revert on the cluster LIFs.

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

Make sure that auto-revert is disabled after running this command.

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

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

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

   `network interface show -vserver Cluster`

   Show example

```
cluster1::*> network interface show -vserver Cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------- ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
cluster1::*>
```

6. Verify that the cluster is healthy:

   `cluster show`

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
cluster1::*>
```

Step 2: Configure and verify the setup

1. 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`

2. Clean the configuration on switch cs2 and perform a basic setup.

   When updating or applying a new RCF, you must erase the switch settings and perform basic configuration. You must be connected to the switch 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. Perform a reboot of the switch:

   Show example

   ```
   (cs2)# reload

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

3. 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

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

4. 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

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

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

Show example

```
cs2# show banner motd

********************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch   : Cisco Nexus 3132Q-V
* Filename : Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
* Date     : Nov-02-2020
* Version  : v1.6
*
* Port Usage : Breakout configuration
* Ports  1- 6: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4,int e1/4/1-4, e1/5/1-4, e1/6/1-4
* Ports  7-30: 40GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
*
* IMPORTANT NOTES
* - Load Nexus_3132QV_RCF_v1.6-Cluster-HA.txt for non breakout
config
*
* - This RCF utilizes QoS and requires specific TCAM configuration,
requiring
*   cluster switch to be rebooted before the cluster becomes
operational.
*
* - Perform the following steps to ensure proper RCF installation:
*
*   (1) Apply RCF, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class
IPv4...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*
*   (4) Save running-configuration again
*
```

```
* - If running NX-OS versions 9.3(5) 9.3(6), 9.3(7), or 9.3(8)
*     - Downgrade the NX-OS firmware to version 9.3(5) or earlier if
*       NX-OS using a version later than 9.3(5).
*     - Do not upgrade NX-OS prior to applying v1.9 RCF file.
*     - After the RCF is applied and switch rebooted, then proceed to
upgrade
*       NX-OS to version 9.3(5) or later.
*
* - If running 9.3(9) 10.2(2) or later the RCF can be applied to the
switch
*       after the upgrade.
*
* - Port 1 multiplexed H/W configuration options:
*      hardware profile front portmode qsfp      (40G H/W port 1/1 is
active - default)
*      hardware profile front portmode sfp-plus  (10G H/W ports 1/1/1
- 1/1/4 are active)
*      hardware profile front portmode qsfp      (To reset to QSFP)
*
********************************************************************
**********
```

6. 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.

   > For steps on how to bring your 10GbE ports online after an upgrade of the RCF, see the Knowledge Base article 10GbE ports on a Cisco 3132Q cluster switch do not come online.

7. 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.

Show example

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

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

Show example

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

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

Show example

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

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

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

    `network port show -ipspace Cluster`

Show example

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

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

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

```
Node: cluster1-04

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

b. Verify the switch health from the cluster.

`network device-discovery show -protocol cdp`

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-C3132Q-V
             e0d    cs2                       Ethernet1/7
N3K-C3132Q-V
cluster01-2/cdp
             e0a    cs1                       Ethernet1/8
N3K-C3132Q-V
             e0d    cs2                       Ethernet1/8
N3K-C3132Q-V
cluster01-3/cdp
             e0a    cs1                       Ethernet1/1/1
N3K-C3132Q-V
             e0b    cs2                       Ethernet1/1/1
N3K-C3132Q-V
cluster1-04/cdp
             e0a    cs1                       Ethernet1/1/2
N3K-C3132Q-V
             e0b    cs2                       Ethernet1/1/2
N3K-C3132Q-V

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

cs2                         cluster-network    10.233.205.91
```

```
N3K-C3132Q-V
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

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

> You might observe the following output on the cs1 switch console depending on the RCF version previously loaded on the switch:
>
> ```
> 2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
> UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
> VLAN0092. Port consistency restored.
> 2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-
> BLOCK_PVID_PEER: Blocking port-channel1 on VLAN0001.
> Inconsistent peer vlan.
> 2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-
> BLOCK_PVID_LOCAL: Blocking port-channel1 on VLAN0092.
> Inconsistent local vlan.
> ```

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

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

Show example

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

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

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

Show example

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     false
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     false
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     false
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     false
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
cluster1::*>
```

13. 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::*>
```

14. Repeat Steps 1 to 10 on switch cs1.
15. Enable auto-revert on the cluster LIFs.

Show example

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

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

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

Step 3: Verify the configuration

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

```
show interface brief | grep 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) --
.
.
```

2. 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#
```

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

`network interface show -vserver Cluster`

Show example

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
cluster1::*>
```

4. 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
cluster1::*>
```

5. 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)
```

6. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting

switch-related log files by using the commands:

`system switch ethernet log setup-password` and

`system switch ethernet log enable-collection`

a. Enter: `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
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>
```

b. Enter: `system switch ethernet log enable-collection`

Show example

```
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.

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

   `system cluster-switch log setup-password` and

   `system cluster-switch log enable-collection`

   a. Enter: `system cluster-switch log setup-password`

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>
```

b. Enter: `system cluster-switch log enable-collection`

Show example

```
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.

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 3132Q-V 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
RSA keys not present	Regenerate ONTAP SSH keys. Contact NetApp support.
switch password error	Verify credentials, test SSH connectivity, and regenerate ONTAP SSH keys. Review the switch documentation or contact NetApp support for instructions.
ECDSA keys not present for FIPS	If FIPS mode is enabled, ECDSA keys need to be generated on the switch before retrying.
pre-existing log found	Remove the previous log collection file on the switch.

switch dump log error	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 3132Q-V 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: cshm1!
                                  Model Number: N3K-C3132Q-V
                                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-C3132Q-V
                                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

Migrate a Cisco Nexus 5596 cluster switch to a Cisco Nexus 3132Q-V cluster switch

Follow this procedure to replace an existing Nexus 5596 cluster switch with a Nexus 3132Q-V cluster switch.

Review requirements

Review the Cisco Nexus 5596 requirements in Requirements for replacing Cisco Nexus 3132Q-V cluster switches.

For more information, see:

- Cisco Ethernet Switch description page
- Hardware Universe

Replace the switch

About the examples

The examples in this procedure describe replacing Nexus 5596 switches with Nexus 3132Q-V switches. You can use these steps (with modifications) to replace other older Cisco switches.

The procedure uses the following switch and node nomenclature:

- The command outputs might vary depending on different releases of ONTAP.
- The Nexus 5596 switches to be replaced are CL1 and CL2.
- The Nexus 3132Q-V switches to replace the Nexus 5596 switches are C1 and C2.
- n1_clus1 is the first cluster logical interface (LIF) connected to cluster switch 1 (CL1 or C1) for node n1.
- n1_clus2 is the first cluster LIF connected to cluster switch 2 (CL2 or C2) for node n1.
- n1_clus3 is the second LIF connected to cluster switch 2 (CL2 or C2) for node n1.
- n1_clus4 is the second LIF connected to cluster switch 1 (CL1 or C1) for node n1.
- The nodes are n1, n2, n3, and n4.
- The examples in this procedure use four nodes: Two nodes use four 10 GbE cluster interconnect ports: e0a, e0b, e0c, and e0d. The other two nodes use two 40/100 GbE cluster interconnect ports: e4a, e4e. The Hardware Universe lists the actual cluster ports on your platforms.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.

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

About this task

This procedure covers the following scenarios:

- The cluster starts with two nodes connected and functioning in a 2 Nexus 5596 cluster switches.
- The cluster switch CL2 to be replaced by C2 (Steps 1 - 19)
    - Traffic on all cluster ports and LIFs on all nodes connected to CL2 are migrated onto the first cluster ports and LIFs connected to CL1.
    - Disconnect cabling from all cluster ports on all nodes connected to CL2, and then use supported break-out cabling to reconnect the ports to new cluster switch C2.
    - Disconnect cabling between ISL ports between CL1 and CL2, and then use supported break-out cabling to reconnect the ports from CL1 to C2.
    - Traffic on all cluster ports and LIFs connected to C2 on all nodes is reverted.
- The cluster switch CL2 to be replaced by C2
    - 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 replacement

To replace an existing Nexus 5596 cluster switch with a Nexus 3132Q-V cluster switch, you must perform a specific sequence of tasks.

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

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device              Interface        Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e0a    CL1                 Ethernet1/1      N5K-C5596UP
            e0b    CL2                 Ethernet1/1      N5K-C5596UP
            e0c    CL2                 Ethernet1/2      N5K-C5596UP
            e0d    CL1                 Ethernet1/2      N5K-C5596UP
n2         /cdp
            e0a    CL1                 Ethernet1/3      N5K-C5596UP
            e0b    CL2                 Ethernet1/3      N5K-C5596UP
            e0c    CL2                 Ethernet1/4      N5K-C5596UP
            e0d    CL1                 Ethernet1/4      N5K-C5596UP
8 entries were displayed.
```

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

   a. Display the network port attributes:

      `network port show`

Show example

The following example displays the network port attributes on a system:

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

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

Node: n2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

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

Show example

The following example displays the general information about all of the LIFs on your system:

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

c. Display information about the discovered cluster switches:
`system cluster-switch show`

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
Model
----------------------------- ------------------ ---------------
---------------
CL1                           cluster-network    10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP
CL2                           cluster-network    10.10.1.102
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP

2 entries were displayed.
```

4. Set the `-auto-revert` parameter to `false` on cluster LIFs clus1 and clus2 on both nodes:

```
network interface modify
```

Show example

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```

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

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

   a. Go to the Cisco Ethernet Switches page on the NetApp Support Site.
   b. Note your switch and the required software versions in the table on that page.
   c. Download the appropriate version of the RCF.
   d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
   e. Download the appropriate version of the image software.

      See the *ONTAP 8.x or later Cluster and Management Network Switch Reference Configuration Files*Download page, and then click the appropriate version.

      To find the correct version, see the *ONTAP 8.x or later Cluster Network Switch Download page*.

6. Migrate the LIFs associated with the second Nexus 5596 switch to be replaced:

   `network interface migrate`

Show example

The following example shows n1 and n2, but LIF migration must be done on all of the nodes:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 –
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 –
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 –
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 –
destination-node n2 -destination-port e0d
```

7. Verify the cluster’s health:

   `network interface show`

Show example

The following example shows the result of the previous `network interface migrate` command:

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

8. Shut down the cluster interconnect ports that are physically connected to switch CL2:

   `network port modify`

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
```

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

   `cluster ping-cluster`

Show example

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

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check
```

10. Shut down the ISL ports 41 through 48 on the active Nexus 5596 switch CL1:

Show example

The following example shows how to shut down ISL ports 41 through 48 on the Nexus 5596 switch CL1:

```
(CL1)# configure
(CL1)(Config)# interface e1/41-48
(CL1)(config-if-range)# shutdown
(CL1)(config-if-range)# exit
(CL1)(Config)# exit
(CL1)#
```

If you are replacing a Nexus 5010 or 5020, specify the appropriate port numbers for ISL.

11. Build a temporary ISL between CL1 and C2.

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
```

Step 2: Configure ports

1. On all nodes, remove all cables attached to the Nexus 5596 switch CL2.

   With supported cabling, reconnect disconnected ports on all nodes to the Nexus 3132Q-V switch C2.

2. Remove all the cables from the Nexus 5596 switch CL2.

   Attach the appropriate Cisco QSFP to SFP+ break-out cables connecting port 1/24 on the new Cisco 3132Q-V switch, C2, to ports 45 to 48 on existing Nexus 5596, CL1.

3. Verify that interfaces eth1/45-48 already have `channel-group 1 mode active` in their running configuration.
4. Bring up ISLs ports 45 through 48 on the active Nexus 5596 switch CL1.

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)#
```

5. Verify that the ISLs are `up` on the Nexus 5596 switch CL1:

`show port-channel summary`

Show example

Ports eth1/45 through eth1/48 should indicate (P) meaning that the ISL ports are `up` in the port-channel:

```
Example
CL1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/41(D)   Eth1/42(D)
Eth1/43(D)
                                    Eth1/44(D)   Eth1/45(P)
Eth1/46(P)
                                    Eth1/47(P)   Eth1/48(P)
```

6. Verify that the ISLs are `up` on the 3132Q-V switch C2:

   `show port-channel summary`

   Show example

   Ports eth1/24/1, eth1/24/2, eth1/24/3, and eth1/24/4 should indicate (P) meaning that the ISL ports are `up` in the port-channel:

```
C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(D)   Eth1/32(D)
2     Po2(SU)      Eth    LACP      Eth1/24/1(P)  Eth1/24/2(P)
Eth1/24/3(P)
                                    Eth1/24/4(P)
```

7. On all nodes, bring up all the cluster interconnect ports connected to the 3132Q-V switch C2:

   `network port modify`

   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
```

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

   `network interface revert`

Show example

The following example shows the migrated cluster LIFs being reverted to their home ports on nodes n1 and n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

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

`network interface show`

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

10. Verify that the clustered ports are connected:

`network port show`

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.
```

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

```
cluster ping-cluster
```

Show example

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

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

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

    `network interface migrate`

    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
    ```

13. Verify the cluster 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:

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

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

14. On all the nodes, shut down the node ports that are connected to CL1:

`network port modify`

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
```

15. Shut down the ISL ports 24, 31, and 32 on the active 3132Q-V switch C2:

    `shutdown`

    Show example

    The following example shows how to shut down ISLs 24, 31, and 32:

    ```
    C2# configure
    C2(Config)# interface e1/24/1-4
    C2(config-if-range)# shutdown
    C2(config-if-range)# exit
    C2(config)# interface 1/31-32
    C2(config-if-range)# shutdown
    C2(config-if-range)# exit
    C2(config-if)# exit
    C2#
    ```

16. On all nodes, remove all cables attached to the Nexus 5596 switch CL1.

    With supported cabling, reconnect disconnected ports on all nodes to the Nexus 3132Q-V switch C1.

17. Remove the QSFP breakout cable from Nexus 3132Q-V C2 ports e1/24.

    Connect ports e1/31 and e1/32 on C1 to ports e1/31 and e1/32 on C2 using supported Cisco QSFP optical fiber or direct-attach cables.

18. Restore the configuration on port 24 and remove the temporary Port Channel 2 on C2:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

19. Bring up ISL ports 31 and 32 on C2, the active 3132Q-V switch: `no shutdown`

Show example

The following example shows how to bring up ISLs 31 and 32 on the 3132Q-V switch C2:

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

Step 3: Verify the configuration

1. Verify that the ISL connections are `up` on the 3132Q-V switch C2:

`show port-channel summary`

Show example

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

```
C1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-         Type   Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)       Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

2. On all nodes, bring up all the cluster interconnect ports connected to the new 3132Q-V 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 3132Q-V switch C1:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

3. Verify the status of the cluster node port:

`network port show`

Show example

The following example verifies that all cluster interconnect ports on all nodes on the new 3132Q-V switch C1 are `up`:

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

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

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-
8 entries were displayed.
```

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

```
network interface revert
```

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
```

5. Verify that the interface is home:

```
network interface show
```

Show example

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

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

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

   `cluster ping-cluster`

Show example

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

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

7. Expand the cluster by adding nodes to the Nexus 3132Q-V cluster switches.
8. 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 3132Q-V cluster switches, and both nodes have joined the cluster. The 40 GbE cluster interconnect ports used are e4a and e4e.

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device              Interface        Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e0a    C1                 Ethernet1/1/1    N3K-
C3132Q-V
            e0b    C2                 Ethernet1/1/1    N3K-
C3132Q-V
            e0c    C2                 Ethernet1/1/2    N3K-
C3132Q-V
            e0d    C1                 Ethernet1/1/2    N3K-
C3132Q-V
n2         /cdp
            e0a    C1                 Ethernet1/1/3    N3K-
C3132Q-V
            e0b    C2                 Ethernet1/1/3    N3K-
C3132Q-V
            e0c    C2                 Ethernet1/1/4    N3K-
C3132Q-V
            e0d    C1                 Ethernet1/1/4    N3K-
C3132Q-V
n3         /cdp
            e4a    C1                 Ethernet1/7      N3K-
C3132Q-V
            e4e    C2                 Ethernet1/7      N3K-
C3132Q-V
n4         /cdp
            e4a    C1                 Ethernet1/8      N3K-
C3132Q-V
            e4e    C2                 Ethernet1/8      N3K-
C3132Q-V
12 entries were displayed.
```

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

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

Node: n2

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

Node: n3

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

```
-

Node: n4

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------- ------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

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

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.104
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

CL1                           cluster-network   10.10.1.101
NX5596
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP
CL2                           cluster-network    10.10.1.102
NX5596
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.1(1)N1(1)
    Version Source: CDP

4 entries were displayed.
```

9. Remove the replaced Nexus 5596 if they are not automatically removed:

   `system cluster-switch delete`

   Show example

   The following example shows how to remove the Nexus 5596:

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

10. Configure clusters clus1 and clus2 to auto revert on each node and confirm.

    Show example

    ```
    cluster::*> network interface modify -vserver node1 -lif clus1 -auto
    -revert true
    cluster::*> network interface modify -vserver node1 -lif clus2 -auto
    -revert true
    cluster::*> network interface modify -vserver node2 -lif clus1 -auto
    -revert true
    cluster::*> network interface modify -vserver node2 -lif clus2 -auto
    -revert true
    ```

11. Verify that the proper cluster switches are monitored:

    `system cluster-switch show`

Show example

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

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.104
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

12. 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.

13. 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 CN1610 cluster switches to Cisco Nexus 3132Q-V cluster switches

Follow this procedure to replace the existing CN1610 cluster switches with Cisco Nexus 3132Q-V cluster switches.

Review requirements

Review the NetApp CN1610 requirements requirements in Requirements for replacing Cisco Nexus 3132Q-V cluster switches.

For more information, see:

- NetApp CN1601 and CN1610 description page
- Cisco Ethernet Switch description page
- Hardware Universe

Replace the switch

Switch and node nomenclature

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

- The command outputs might vary depending on different releases of ONTAP software.
- The CN1610 switches to be replaced are CL1 and CL2.
- The Nexus 3132Q-V switches to replace the CN1610 switches are C1 and C2.
- n1_clus1 is the first cluster logical interface (LIF) that is connected to cluster switch 1 (CL1 or C1) for node n1.
- n1_clus2 is the first cluster LIF that is connected to cluster switch 2 (CL2 or C2) for node n1.
- n1_clus3 is the second LIF that is connected to cluster switch 2 (CL2 or C2) for node n1.
- n1_clus4 is the second LIF that is connected to cluster switch 1 (CL1 or C1) for node n1.
- The nodes are n1, n2, n3, and n4.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.

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 40/100 GbE cluster interconnect fiber cables: e4a and e4e.

The Hardware Universe has information about the cluster fiber cables on your platforms.

About this task

This procedure covers the following scenario:

- The cluster starts with two nodes connected to two CN1610 cluster switches.
- Cluster switch CL2 to be replaced by C2
  - Traffic on all cluster ports and LIFs on all nodes connected to CL2 are migrated onto the first cluster ports and LIFs connected to CL1.

◦ Disconnect cabling from all cluster ports on all nodes connected to CL2, and then use supported breakout cabling to reconnect the ports to new cluster switch C2.
◦ Disconnect cabling between ISL ports CL1 and CL2, and then use supported breakout cabling to reconnect the ports from CL1 to C2.
◦ Traffic on all cluster ports and LIFs connected to C2 on all nodes is reverted.

- Cluster switch CL1 to be replaced by C1
  ◦ Traffic on all cluster ports and LIFs on all nodes connected to CL1 are migrated onto the second cluster ports and LIFs connected to C2.
  ◦ Disconnect cabling from all cluster ports on all nodes connected to CL1, and then use supported breakout cabling to reconnect the ports to new cluster switch C1.
  ◦ Disconnect cabling between ISL ports CL1 and C2, and then use supported breakout cabling to reconnect the ports from C1 to C2.
  ◦ Traffic on all migrated cluster ports and LIFs connected to C1 on all nodes is reverted.

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

Step 1: Prepare for replacement

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

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

       Local  Discovered
Node   Port   Device       Interface   Platform
------ ------ ------------ ----------- ----------
n1     /cdp
        e0a   CL1          0/1         CN1610
        e0b   CL2          0/1         CN1610
        e0c   CL2          0/2         CN1610
        e0d   CL1          0/2         CN1610
n2     /cdp
        e0a   CL1          0/3         CN1610
        e0b   CL2          0/3         CN1610
        e0c   CL2          0/4         CN1610
        e0d   CL1          0/4         CN1610

8 entries were displayed.
```

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

   a. Display the cluster network port attributes:

      `network port show`

Show example

The following example displays the network port attributes on a system:

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

Node: n1
                Broadcast                Speed (Mbps) Health Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status Health
Status
----- --------- ---------- ----- ----- ------------ ------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -         -
e0b   cluster   cluster    up    9000  auto/10000     -         -
e0c   cluster   cluster    up    9000  auto/10000     -         -
e0d   cluster   cluster    up    9000  auto/10000     -         -

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

8 entries were displayed.
```

b. Display information about the logical interfaces: + `network interface show`

Show example

The following example displays the general information about all of the LIFs on your system:

```
cluster::*> network interface show -role Cluster
       (network interface show)

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

8 entries were displayed.
```

c. Display information about the discovered cluster switches:

`system cluster-switch show`

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
Model
-----------------------------    ---------------- -------------
--------
CL1                              cluster-network  10.10.1.101
CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

CL2                              cluster-network  10.10.1.102
CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

2 entries were displayed.
```

4. Set the `-auto-revert` parameter to false on cluster LIFs clus1 and clus4 on both nodes:

`network interface modify`

Show example

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus4 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus4 -auto
-revert false
```

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

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

   a. See the Cisco Ethernet Switches page on NetApp Support Site.
   b. Note your switch and the required software versions in the table on that page.
   c. Download the appropriate version of the RCF.
   d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
   e. Download the appropriate version of the image software.

      Cisco® Cluster and Management Network Switch Reference Configuration File Download

6. Migrate the LIFs associated with the second CN1610 switch to be replaced:

   `network interface migrate`

   > You must migrate the cluster LIFs from a connection to the node, either through the service processor or node management interface, which owns the cluster LIF being migrated.

   Show example

   The following example shows n1 and n2, but LIF migration must be done on all the nodes:

   ```
   cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
   -destination-node  n1  -destination-port  e0a
   cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
   -destination-node  n1  -destination-port  e0d
   cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
   -destination-node  n2  -destination-port  e0a
   cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
   -destination-node  n2  -destination-port  e0d
   ```

7. Verify the cluster's health:

   `network interface show`

Show example

The following example shows the result of the previous `network interface migrate` command:

```
cluster::*> network interface show -role Cluster
       (network interface show)

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

8 entries were displayed.
```

8. Shut down the cluster interconnect ports that are physically connected to switch CL2:

`network port modify`

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
```

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

`cluster ping-cluster`

Show example

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

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

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

`shutdown`

Show example

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

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

11. Build a temporary ISL between CL1 and C2:

Show example

The following example builds a temporary ISL between CL1 (ports 13-16) and C2 (ports e1/24/1-4):

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

Step 2: Configure ports

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

   With supported cabling, you must reconnect the disconnected ports on all of the nodes to the Nexus 3132Q-V switch C2.

2. Remove four ISL cables from ports 13 to 16 on the CN1610 switch CL1.

   You must attach appropriate Cisco QSFP to SFP+ breakout cables connecting port 1/24 on the new Cisco 3132Q-V switch C2, to ports 13 to 16 on existing CN1610 switch CL1.

> ⓘ When reconnecting any cables to the new Cisco 3132Q-V switch, you must use either optical fiber or Cisco twinax cables.

3. To make the ISL dynamic, configure the ISL interface 3/1 on the active CN1610 switch to disable the static mode: `no port-channel static`

   This configuration matches with the ISL configuration on the 3132Q-V switch C2 when the ISLs are brought up on both switches in step 11

   Show example

   The following example shows the configuration of the ISL interface 3/1 using the `no port-channel static` command to make the ISL dynamic:

   ```
   (CL1)# configure
   (CL1)(Config)# interface 3/1
   (CL1)(Interface 3/1)# no port-channel static
   (CL1)(Interface 3/1)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

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

   Show example

   The following example illustrates the process of bringing up ISL ports 13 through 16 on the port-channel interface 3/1:

   ```
   (CL1)# configure
   (CL1)(Config)# interface 0/13-0/16,3/1
   (CL1)(Interface 0/13-0/16,3/1)# no shutdown
   (CL1)(Interface 0/13-0/16,3/1)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

5. Verify that the ISLs are `up` on the CN1610 switch CL1:

   `show port-channel`

   The "Link State" should be `Up`, "Type" should be `Dynamic`, and the "Port Active" column should be `True` for ports 0/13 to 0/16:

Show example

```
(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
```

6. Verify that the ISLs are `up` on the 3132Q-V switch C2:

`show port-channel summary`

Show example

Ports Eth1/24/1 through Eth1/24/4 should indicate `(P)`, meaning that all four ISL ports are up in the port-channel. Eth1/31 and Eth1/32 should indicate `(D)` as they are not connected:

```
C2# show port-channel summary

Flags:  D - Down         P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
----------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
----------
1     Po1(SU)     Eth      LACP      Eth1/31(D)   Eth1/32(D)
2     Po2(SU)     Eth      LACP      Eth1/24/1(P) Eth1/24/2(P)
Eth1/24/3(P)
                                     Eth1/24/4(P)
```

7. Bring up all of the cluster interconnect ports that are connected to the 3132Q-V switch C2 on all of the nodes:

   `network port modify`

   Show example

   The following example shows how to bring up the cluster interconnect ports connected to the 3132Q-V switch C2:

   ```
   cluster::*> network port modify -node n1 -port e0b -up-admin true
   cluster::*> network port modify -node n1 -port e0c -up-admin true
   cluster::*> network port modify -node n2 -port e0b -up-admin true
   cluster::*> network port modify -node n2 -port e0c -up-admin true
   ```

8. Revert all of the migrated cluster interconnect LIFs that are connected to C2 on all of the nodes:

   `network interface revert`

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
```

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

   `network interface show`

Show example

The following example shows that the LIFs on clus2 are reverted to their home ports, and shows that the LIFs are successfully reverted if the ports in the "Current Port" column have a status of `true` in the "Is Home" column. If the Is Home value is `false`, then the LIF is not reverted.

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

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

8 entries were displayed.
```

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

    `network port show`

Show example

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

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

Node: n1
                Broadcast               Speed (Mbps) Health   Ignore
Port  IPspace   Domain      Link  MTU   Admin/Open   Status   Health
Status
----- --------- ----------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster     up    9000  auto/10000     -        -
e0b   cluster   cluster     up    9000  auto/10000     -        -
e0c   cluster   cluster     up    9000  auto/10000     -        -
e0d   cluster   cluster     up    9000  auto/10000     -        -

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

8 entries were displayed.
```

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

    `cluster ping-cluster`

Show example

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

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

12. On each node in the cluster, migrate the interfaces that are associated with the first CN1610 switch CL1, to

be replaced:

`network interface migrate`

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
-destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-destination-node n2 -destination-port e0c
```

13. Verify the cluster status:

`network interface show`

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
         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.
```

14. Shut down the node ports that are connected to CL1 on all of the nodes:

`network port modify`

Show example

The following example shows how to shut down the specified ports on nodes n1 and n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

15. Shut down the ISL ports 24, 31, and 32 on the active 3132Q-V switch C2:

    `shutdown`

    Show example

    The following example shows how to shut down ISLs 24, 31, and 32 on the active 3132Q-V switch C2:

    ```
    C2# configure
    C2(config)# interface ethernet 1/24/1-4
    C2(config-if-range)# shutdown
    C2(config-if-range)# exit
    C2(config)# interface ethernet 1/31-32
    C2(config-if-range)# shutdown
    C2(config-if-range)# exit
    C2(config)# exit
    C2#
    ```

16. Remove the cables that are attached to the CN1610 switch CL1 on all of the nodes.

    With supported cabling, you must reconnect the disconnected ports on all of the nodes to the Nexus 3132Q-V switch C1.

17. Remove the QSFP cables from Nexus 3132Q-V C2 port e1/24.

    You must connect ports e1/31 and e1/32 on C1 to ports e1/31 and e1/32 on C2 using supported Cisco QSFP optical fiber or direct-attach cables.

18. Restore the configuration on port 24 and remove the temporary port-channel 2 on C2, by copying the `running-configuration` file to the `startup-configuration` file.

Show example

The following example copies the `running-configuration` file to the `startup-configuration` file:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# interface e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[########################################] 100%
Copy Complete.
```

19. Bring up ISL ports 31 and 32 on C2, the active 3132Q-V switch:

```
no shutdown
```

Show example

The following example shows how to bring up ISLs 31 and 32 on the 3132Q-V switch C2:

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

Step 3: Verify the configuration

1. Verify that the ISL connections are `up` on the 3132Q-V switch C2:

```
show port-channel summary
```

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

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)
```

2. Bring up all of the cluster interconnect ports connected to the new 3132Q-V switch C1 on all of the nodes:

   `network port modify`

   Show example

   The following example shows how to bring up all of the cluster interconnect ports connected to the new 3132Q-V switch C1:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

3. Verify the status of the cluster node port:

   `network port show`

Show example

The following example verifies that all of the cluster interconnect ports on n1 and n2 on the new 3132Q-V switch C1 are `up`:

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

Node: n1
                Broadcast              Speed (Mbps) Health   Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status   Health
Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -        -
e0b   cluster   cluster    up    9000  auto/10000     -        -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -

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

8 entries were displayed.
```

4. Revert all of the migrated cluster interconnect LIFs that were originally connected to C1 on all of the nodes:

`network interface revert`

Show example

The following example shows how to revert the migrated cluster LIFs to their home ports:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

5. Verify that the interface is now home:

   `network interface show`

Show example

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

```
cluster::*> network interface show -role Cluster
       (network interface show)

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

8 entries were displayed.
```

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

```
cluster ping-cluster
```

Show example

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

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1       e0a    10.10.0.1
Cluster n1_clus2 n1       e0b    10.10.0.2
Cluster n1_clus3 n1       e0c    10.10.0.3
Cluster n1_clus4 n1       e0d    10.10.0.4
Cluster n2_clus1 n2       e0a    10.10.0.5
Cluster n2_clus2 n2       e0b    10.10.0.6
Cluster n2_clus3 n2       e0c    10.10.0.7
Cluster n2_clus4 n2       e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

7. Expand the cluster by adding nodes to the Nexus 3132Q-V cluster switches.

8. 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 3132Q-V cluster switches, and both nodes have joined the cluster. The 40 GbE cluster interconnect ports used are e4a and e4e.

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

       Local  Discovered
Node   Port   Device       Interface       Platform
------ ------ ------------ --------------- -------------
n1     /cdp
        e0a   C1           Ethernet1/1/1   N3K-C3132Q-V
        e0b   C2           Ethernet1/1/1   N3K-C3132Q-V
        e0c   C2           Ethernet1/1/2   N3K-C3132Q-V
        e0d   C1           Ethernet1/1/2   N3K-C3132Q-V
n2     /cdp
        e0a   C1           Ethernet1/1/3   N3K-C3132Q-V
        e0b   C2           Ethernet1/1/3   N3K-C3132Q-V
        e0c   C2           Ethernet1/1/4   N3K-C3132Q-V
        e0d   C1           Ethernet1/1/4   N3K-C3132Q-V
n3     /cdp
        e4a   C1           Ethernet1/7     N3K-C3132Q-V
        e4e   C2           Ethernet1/7     N3K-C3132Q-V
n4     /cdp
        e4a   C1           Ethernet1/8     N3K-C3132Q-V
        e4e   C2           Ethernet1/8     N3K-C3132Q-V

12 entries were displayed.
```

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

Node: n1
                Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e0a   cluster   cluster    up    9000  auto/10000     -        -
e0b   cluster   cluster    up    9000  auto/10000     -        -
e0c   cluster   cluster    up    9000  auto/10000     -        -
e0d   cluster   cluster    up    9000  auto/10000     -        -
```

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

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

Node: n4
                Broadcast              Speed (Mbps) Health
Ignore
Port  IPspace   Domain     Link  MTU   Admin/Open   Status
Health Status
----- --------- ---------- ----- ----- ------------ --------
-------------
e4a   cluster   cluster    up    9000  auto/40000     -         -
e4e   cluster   cluster    up    9000  auto/40000     -         -

12 entries were displayed.
```

```
cluster::*> network interface show -role Cluster
       (network interface show)

         Logical    Status      Network        Current  Current
Is
Vserver  Interface  Admin/Oper  Address/Mask   Node     Port
Home
-------- ---------- ----------- -------------- -------- --------
-----
Cluster
         n1_clus1   up/up       10.10.0.1/24   n1       e0a
true
         n1_clus2   up/up       10.10.0.2/24   n1       e0b
true
         n1_clus3   up/up       10.10.0.3/24   n1       e0c
true
         n1_clus4   up/up       10.10.0.4/24   n1       e0d
true
         n2_clus1   up/up       10.10.0.5/24   n2       e0a
true
         n2_clus2   up/up       10.10.0.6/24   n2       e0b
true
         n2_clus3   up/up       10.10.0.7/24   n2       e0c
true
         n2_clus4   up/up       10.10.0.8/24   n2       e0d
true
         n3_clus1   up/up       10.10.0.9/24   n3       e4a
true
         n3_clus2   up/up       10.10.0.10/24  n3       e4e
true
         n4_clus1   up/up       10.10.0.11/24  n4       e4a
true
         n4_clus2   up/up       10.10.0.12/24  n4       e4e
true

12 entries were displayed.
```

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

Switch                      Type             Address       Model
--------------------------- ---------------- -------------
---------
C1                          cluster-network  10.10.1.103
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network  10.10.1.104
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

CL1                         cluster-network  10.10.1.101   CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

CL2                         cluster-network  10.10.1.102
CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.2.0.7
    Version Source: ISDP

4 entries were displayed.
```

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

`system cluster-switch delete`

Show example

The following example shows how to remove the CN1610 switches:

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

10. Configure clusters clus1 and clus4 to `-auto-revert` on each node and confirm:

Show example

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus4 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus4 -auto
-revert true
```

11. Verify that the proper cluster switches are monitored:

```
system cluster-switch show
```

Show example

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

Switch                          Type                Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network    10.10.1.104
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

12. 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.

13. 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 switchless cluster to a two-node switched cluster

If you have a two-node switchless cluster, you can follow this procedure to migrate to a two-node switched cluster that includes Cisco Nexus 3132Q-V cluster network switches. The replacement procedure is a nondisruptive procedure (NDO).

Review requirements

Ports and node connections

Make sure you understand the port and node connections and cabling requirements when you migrate to a two-node switched cluster with Cisco Nexus 3132Q-V cluster switches.

- The cluster switches use the Inter-Switch Link (ISL) ports e1/31-32.
- The Hardware Universe contains information about supported cabling to Nexus 3132Q-V switches:
  - The nodes with 10 GbE cluster connections require QSFP optical modules with breakout fiber cables or QSFP to SFP+ copper break-out cables.
  - The nodes with 40/100 GbE cluster connections require supported QSFP/QSFP28 optical modules with fiber cables or QSFP/QSFP28 copper direct-attach cables.
  - The cluster switches use the appropriate ISL cabling: 2x QSFP28 fiber or copper direct-attach cables.
- On Nexus 3132Q-V, you can operate QSFP ports as either 40/100 Gb Ethernet or 4 x10 Gb Ethernet modes.

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

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

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

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

- Make sure you configured some of the ports on Nexus 3132Q-V to run at 10 GbE or 40/100 GbE.

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

- 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.

What you'll need

- Configurations properly set up and functioning.
- Nodes running ONTAP 9.4 or later.

- All cluster ports in the `up` state.
- The Cisco Nexus 3132Q-V cluster switch is supported.
- The existing cluster network configuration has:
  - The Nexus 3132 cluster infrastructure that is redundant and fully functional on both switches.
  - The latest RCF and NX-OS versions on your switches.

    The Cisco Ethernet Switches page has information about the ONTAP and NX-OS versions supported in this procedure.
  - Management connectivity on both switches.
  - Console access to both switches.
  - All cluster logical interfaces (LIFs) in the `up` state without being migrated.
  - Initial customization of the switch.
  - All the ISL ports enabled and cabled.

In addition, you must plan, migrate, and read the required documentation on 10 GbE and 40/100 GbE connectivity from nodes to Nexus 3132Q-V cluster switches.

Migrate the switches

About the examples

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

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

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

About this task

This procedure covers the following scenarios:

- n1_clus1 is the first cluster logical interface (LIF) to be connected to cluster switch C1 for node n1.
- n1_clus2 is the first cluster LIF to be connected to cluster switch C2 for node n1.
- n2_clus1 is the first cluster LIF to be connected to cluster switch C1 for node n2.
- n2_clus2 is the second cluster LIF to be connected to cluster switch C2 for node n2.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco ® Cluster Network Switch Reference Configuration File Download page.

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

- The cluster starts with two nodes connected and functioning in a two-node switchless cluster setting.
- The first cluster port is moved to C1.
- The second cluster port is moved to C2.

* The two-node switchless cluster option is disabled.

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

   a. Display the network port attributes:

      ```
      network port show
      ```

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.
```

b. Display information about the logical interfaces:

`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
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

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

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

   a. Go to the Cisco Ethernet Switches page on the NetApp Support Site.
   b. Note your switch and the required software versions in the table on that page.
   c. Download the appropriate version of RCF.
   d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
   e. Download the appropriate version of the image software.

4. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.

Step 2: Move first cluster port to C1

1. On Nexus 3132Q-V switches C1 and C2, disable all node-facing ports C1 and C2, but do not disable the ISL ports.

Show example

The following example shows ports 1 through 30 being disabled on Nexus 3132Q-V cluster switches C1 and C2 using a configuration supported in RCF `NX3132_RCF_v1.1_24p10g_26p40g.txt`:

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

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

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

```
show port-channel summary
```

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)

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)
```

4. Display the list of neighboring devices on the switch:

```
show cdp neighbors
```

Show example

```
C1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C2                 Eth1/31        174    R S I s     N3K-C3132Q-V
Eth1/31
C2                 Eth1/32        174    R S I s     N3K-C3132Q-V
Eth1/32

Total entries displayed: 2

C2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C1                 Eth1/31        178    R S I s     N3K-C3132Q-V
Eth1/31
C1                 Eth1/32        178    R S I s     N3K-C3132Q-V
Eth1/32

Total entries displayed: 2
```

5. Display the cluster port connectivity on each node:

```
network device-discovery show
```

Show example

The following example shows a two-node switchless cluster configuration.

```
cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device              Interface        Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e4a    n2                  e4a              FAS9000
            e4e    n2                  e4e              FAS9000
n2         /cdp
            e4a    n1                  e4a              FAS9000
            e4e    n1                  e4e              FAS9000
```

6. Migrate the clus1 interface to the physical port hosting clus2:

   `network interface migrate`

   Execute this command from each local node.

   Show 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
```

7. Verify the cluster interfaces migration:

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

8. Shut down cluster ports clus1 LIF on both nodes:

   `network port modify`

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

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

   `cluster ping-cluster`

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 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

10. Disconnect the cable from e4a on node n1.

    You can refer to the running configuration and connect the first 40 GbE port on the switch C1 (port 1/7 in this example) to e4a on n1 using supported cabling on Nexus 3132Q-V.

    When reconnecting any cables to a new Cisco cluster switch, the cables used must be either fiber or cabling supported by Cisco.

11. 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.

12. Enable all node-facing ports on C1.

Show example

The following example shows ports 1 through 30 being enabled on Nexus 3132Q-V cluster switches C1 and C2 using the configuration supported in RCF `NX3132_RCF_v1.1_24p10g_26p40g.txt`:

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

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

`network port modify`

Show example

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

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

`network port show`

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.
```

15. 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_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
```

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

    `network interface show`

    The `Is Home` column should display a value of `true` for all of the ports listed in the `Current Port` column. If the displayed value is `false`, the port has not been reverted.

    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 3: Move second cluster port to C2

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-C3132Q-V
            e4e    n2                  e4e              FAS9000
n2         /cdp
            e4a    C1                  Ethernet1/8      N3K-C3132Q-V
            e4e    n1                  e4e              FAS9000
```

2. On the console of each node, migrate clus2 to port e4a:

   `network interface migrate`

   Show 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`

   The following example shows the specified ports being shut down on both nodes:

```
  cluster::*> network port modify -node n1 -port e4e -up-admin false
  cluster::*> network port modify -node n2 -port e4e -up-admin false
```

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 the switch C2 (port 1/7 in this example) to e4e on n1 using supported cabling on Nexus 3132Q-V.

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 supported cabling.

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 `NX3132_RCF_v1.1_24p10g_26p40g.txt`:

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

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

   `network port modify`

   The following example shows the specified ports being brought up:

   ```
   cluster::*> network port modify -node n1 -port e4e -up-admin true
   cluster::*> network port modify -node n2 -port e4e -up-admin true
   ```

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

   `network interface revert`

   The following example shows the migrated LIFs being reverted to their home ports.

   ```
   cluster::*> network interface revert -vserver Cluster -lif n1_clus2
   cluster::*> network interface revert -vserver Cluster -lif n2_clus2
   ```

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

    `network interface show`

    The `Is Home` column should display a value of `true` for all of the ports listed in the `Current Port` column. If the displayed value is `false`, the port has not been reverted.

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.
```

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

```
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.
```

Step 4: Disable the two-node switchless cluster option

1. Display the cluster switch port numbers each cluster port is connected to 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-C3132Q-V
            e4e    C2                  Ethernet1/7      N3K-C3132Q-V
n2         /cdp
            e4a    C1                  Ethernet1/8      N3K-C3132Q-V
            e4e    C2                  Ethernet1/8      N3K-C3132Q-V
```

2. Display discovered and monitored cluster switches:

`system cluster-switch show`

Show example

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

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                         cluster-network     10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

3. Disable the two-node switchless configuration settings on any node:

   `network options switchless-cluster`

```
network options switchless-cluster modify -enabled false
```

4. Verify that the `switchless-cluster` option has been disabled.

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

Step 5: Verify the configuration

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

   `cluster ping-cluster`

   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 1500 byte MTU on 32 path(s):
       Local 10.10.0.1 to Remote 10.10.0.3
       Local 10.10.0.1 to Remote 10.10.0.4
       Local 10.10.0.2 to Remote 10.10.0.3
       Local 10.10.0.2 to Remote 10.10.0.4
   Larger than PMTU communication succeeds on 4 path(s)
   RPC status:
   1 paths up, 0 paths down (tcp check)
   1 paths up, 0 paths down (ucp check)
   ```

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>

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.

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`

Replace switches

Requirements for replacing Cisco Nexus 3132Q-V cluster switches

Make sure you understand the configuration requirements, port connections, and cabling requirements when you replace cluster switches.

Cisco Nexus 3132Q-V requirements

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

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

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

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

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

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

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

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

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

Cisco Nexus 5596 requirements

- The following cluster switches are supported:
  - Nexus 5596
  - Nexus 3132Q-V
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.
- The cluster switches use the following ports for connections to nodes:
  - Ports e1/1-40 (10 GbE): Nexus 5596
  - Ports e1/1-30 (40/100 GbE): Nexus 3132Q-V
- The cluster switches use the following Inter-Switch Link (ISL) ports:
  - Ports e1/41-48 (10 GbE): Nexus 5596
  - Ports e1/31-32 (40/100 GbE): Nexus 3132Q-V
- The Hardware Universe contains information about supported cabling to Nexus 3132Q-V switches:
  - Nodes with 10 GbE cluster connections require QSFP to SFP+ optical fiber breakout cables or QSFP to SFP+ copper breakout cables.
  - Nodes with 40/100 GbE cluster connections require supported QSFP/QSFP28optical modules with fiber cables or QSFP/QSFP28 copper direct-attach cables.
- The cluster switches use the appropriate ISL cabling:
  - Beginning: Nexus 5596 to Nexus 5596 (SFP+ to SFP+)
    - 8x SFP+ fiber or copper direct-attach cables
  - Interim: Nexus 5596 to Nexus 3132Q-V (QSFP to 4xSFP+ break-out)
    - 1x QSFP to SFP+ fiber break-out or copper break-out cables
  - Final: Nexus 3132Q-V to Nexus 3132Q-V (QSFP28 to QSFP28)
    - 2x QSFP28 fiber or copper direct-attach cables
- On Nexus 3132Q-V switches, you can operate QSFP/QSFP28 ports as either 40/100 Gigabit Ethernet or 4 x10 Gigabit Ethernet modes.

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

- On the left side of Nexus 3132Q-V switches is a set of 4 SFP+ ports multiplexed to that QSFP28 port.

  By default, the RCF is structured to use the QSFP28 port.

  > You can make 4x SFP+ ports active instead of a QSFP port for Nexus 3132Q-V switches by using the `hardware profile front portmode sfp-plus` command. Similarly, you can reset Nexus 3132Q-V switches to use a QSFP port instead of 4x SFP+ ports by using the `hardware profile front portmode qsfp` command.

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

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

* You have done the planning, migration, and read the required documentation on 10 GbE and 40/100 GbE connectivity from nodes to Nexus 3132Q-V cluster switches.
* The ONTAP and NX-OS versions supported in this procedure are on the Cisco Ethernet Switches page.

NetApp CN1610 requirements

* The following cluster switches are supported:
  * NetApp CN1610
  * Cisco Nexus 3132Q-V
* The cluster switches support the following node connections:
  * NetApp CN1610: ports 0/1 through 0/12 (10 GbE)
  * Cisco Nexus 3132Q-V: ports e1/1-30 (40/100 GbE)
* The cluster switches use the following inter-switch link (ISL) ports:
  * NetApp CN1610: ports 0/13 through 0/16 (10 GbE)
  * Cisco Nexus 3132Q-V: ports e1/31-32 (40/100 GbE)
* The Hardware Universe contains information about supported cabling to Nexus 3132Q-V switches:
  * Nodes with 10 GbE cluster connections require QSFP to SFP+ optical fiber breakout cables or QSFP to SFP+ copper breakout cables
  * Nodes with 40/100 GbE cluster connections require supported QSFP/QSFP28 optical modules with optical fiber cables or QSFP/QSFP28 copper direct-attach cables
* The appropriate ISL cabling is as follows:
  * Beginning: For CN1610 to CN1610 (SFP+ to SFP+), four SFP+ optical fiber or copper direct-attach cables
  * Interim: For CN1610 to Nexus 3132Q-V (QSFP to four SFP+ breakout), one QSFP to SFP+ optical fiber or copper breakout cable
  * Final: For Nexus 3132Q-V to Nexus 3132Q-V (QSFP28 to QSFP28), two QSFP28 optical fiber or copper direct-attach cables
* NetApp twinax cables are not compatible with Cisco Nexus 3132Q-V switches.

  If your current CN1610 configuration uses NetApp twinax cables for cluster-node-to-switch connections or ISL connections and you want to continue using twinax in your environment, you need to procure Cisco twinax cables. Alternatively, you can use optical fiber cables for both the ISL connections and the cluster-node-to-switch connections.

* On Nexus 3132Q-V switches, you can operate QSFP/QSFP28 ports as either 40/100 Gb Ethernet or 4x 10 Gb Ethernet modes.

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

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

  By default, the reference configuration file (RCF) is structured to use the first QSFP port.

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

  > When you use the first four SFP+ ports, it will disable the first 40GbE QSFP port.

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

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

- You must have done the planning, migration, and read the required documentation on 10 GbE and 40/100 GbE connectivity from nodes to Nexus 3132Q-V cluster switches.
- The ONTAP and NX-OS versions that are supported in this procedure are listed on the Cisco Ethernet Switches page.
- The ONTAP and FASTPATH versions that are supported in this procedure are listed on the NetApp CN1601 and CN1610 Switches page.

Replace Cisco Nexus 3132Q-V cluster switches

Follow this procedure to replace a defective Cisco Nexus 3132Q-V switch in a cluster network. The replacement procedure is a nondisruptive procedure (NDO).

Review requirements

Switch requirements

Review the Requirements for replacing Cisco Nexus 3132Q-V cluster switches.

What you'll need

- The existing cluster and network configuration has:
  - The Nexus 3132Q-V cluster infrastructure is redundant and fully functional on both switches.

    The Cisco Ethernet Switch page has the latest RCF and NX-OS versions on your switches.

  - All cluster ports are in the `up` state.
  - Management connectivity exists on both switches.
  - All cluster logical interfaces (LIFs) are in the `up` state and have been migrated.
- For the Nexus 3132Q-V replacement switch, make sure that:

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

Replace the switch

This procedure replaces the second Nexus 3132Q-V cluster switch CL2 with new 3132Q-V switch C2.

About the examples

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

- n1_clus1 is the first cluster logical interface (LIF) connected to cluster switch C1 for node n1.
- n1_clus2 is the first cluster LIF connected to cluster switch CL2 or C2, for node n1.
- n1_clus3 is the second LIF connected to cluster switch C2, for node n1.
- n1_clus4 is the second LIF connected to cluster switch CL1, for node n1.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Cluster Network Switch Reference Configuration File Download page.
- The nodes are n1, n2, n3, and n4. - The examples in this procedure use four nodes: Two nodes use four 10 GB cluster interconnect ports: e0a, e0b, e0c, and e0d. The other two nodes use two 40 GB cluster interconnect ports: e4a and e4e. See the Hardware Universe for the actual cluster ports on your platforms.

About this task

This procedure covers the following scenario:

- The cluster starts with four nodes connected to two Nexus 3132Q-V cluster switches, CL1 and CL2.
- Cluster switch CL2 is to be replaced by C2
    ◦ On each node, cluster LIFs connected to CL2 are migrated onto cluster ports connected to CL1.
    ◦ Disconnect cabling from all ports on CL2 and reconnect cabling to the same ports on the replacement switch C2.
    ◦ On each node, its migrated cluster LIFs are reverted.

Step 1: Prepare for replacement

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
            Local  Discovered
Node        Port   Device              Interface        Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e0a    CL1                 Ethernet1/1/1    N3K-C3132Q-V
            e0b    CL2                 Ethernet1/1/1    N3K-C3132Q-V
            e0c    CL2                 Ethernet1/1/2    N3K-C3132Q-V
            e0d    CL1                 Ethernet1/1/2    N3K-C3132Q-V
n2         /cdp
            e0a    CL1                 Ethernet1/1/3    N3K-C3132Q-V
            e0b    CL2                 Ethernet1/1/3    N3K-C3132Q-V
            e0c    CL2                 Ethernet1/1/4    N3K-C3132Q-V
            e0d    CL1                 Ethernet1/1/4    N3K-C3132Q-V
n3         /cdp
            e4a    CL1                 Ethernet1/7      N3K-C3132Q-V
            e4e    CL2                 Ethernet1/7      N3K-C3132Q-V
n4         /cdp
            e4a    CL1                 Ethernet1/8      N3K-C3132Q-V
            e4e    CL2                 Ethernet1/8      N3K-C3132Q-V

12 entries were displayed
```

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

      `network port show`

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

b. Display information about the logical interfaces:

```
network interface show
```

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
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e0a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e0e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e0a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e0e     true

12 entries were displayed.
```

c. Display the information on the discovered cluster switches:

```
system cluster-switch show
```

Show example

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

Switch                          Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                              cluster-network   10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

CL2                              cluster-network   10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

4. Verify that the appropriate RCF and image are installed on the new Nexus 3132Q-V switch as necessary for your requirements, and make any essential site customizations.

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

   a. On the NetApp Support Site, go to the Cisco Ethernet Switch page.
   b. Note your switch and the required software versions in the table on that page.
   c. Download the appropriate version of the RCF.
   d. Click **CONTINUE** on the **Description** page, accept the license agreement, and then follow the instructions on the **Download** page to download the RCF.
   e. Download the appropriate version of the image software.
5. Migrate the LIFs associated to the cluster ports connected to switch C2:

   `network interface migrate`

Show example

This example shows that the LIF migration is done on all the nodes:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 –destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 –destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 –destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 –destination-node n2 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2
-source-node n3 –destination-node n3 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2
-source-node n4 –destination-node n4 -destination-port e4a
```

6. Verify cluster's health:

`network interface show`

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
12 entries were displayed.
```

7. Shut down the cluster interconnect ports that are physically connected to switch CL2:

`network port modify`

Show example

This example shows the specified ports being shut down on all nodes:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

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

   `cluster ping-cluster`

Show example

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8
Cluster n3_clus1 n4     e0a 10.10.0.9
Cluster n3_clus2 n3     e0e 10.10.0.10
Cluster n4_clus1 n4     e0a 10.10.0.11
Cluster n4_clus2 n4     e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
```

```
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12

Larger than PMTU communication succeeds on 32 path(s)
RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

9. Shut down the ports 1/31 and 1/32 on CL1, and the active Nexus 3132Q-V switch:

   `shutdown`

   Show example

   This example shows the ISL ports 1/31 and 1/32 being shut down on switch CL1:

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

Step 2: Configure ports

1. Remove all the cables attached to the Nexus 3132Q-V switch CL2 and reconnect them to the replacement switch C2 on all nodes.
2. Remove the ISL cables from ports e1/31 and e1/32 on CL2 and reconnect them to the same ports on the replacement switch C2.
3. Bring up ISLs ports 1/31 and 1/32 on the Nexus 3132Q-V switch CL1:

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

4. Verify that the ISLs are up on CL1:

   `show port-channel`

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

   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)
```

5. Verify that the ISLs are up on C2:

   `show port-channel summary`

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

Show example

```
C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

6. On all nodes, bring up all the cluster interconnect ports connected to the Nexus 3132Q-V switch C2:

`network port modify`

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
```

7. For all nodes, revert all of the migrated cluster interconnect LIFs:

`network interface revert`

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
Cluster::*> network interface revert –vserver Cluster –lif n3_clus2
Cluster::*> network interface revert –vserver Cluster –lif n4_clus2
```

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

`network interface show`

Show example

This example shows that all the LIFs are successfully reverted because the ports listed under the `Current Port` column have a status of `true` in the `Is Home` column. If the `Is Home` column value is `false`, the LIF has not been reverted.

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

9. Verify that the cluster ports are connected:

`network port show`

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

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

```
cluster ping-cluster
```

Show example

```
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 3: Verify the configuration

1. 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
            Local  Discovered
Node        Port   Device              Interface        Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e0a    C1                 Ethernet1/1/1    N3K-C3132Q-V
            e0b    C2                 Ethernet1/1/1    N3K-C3132Q-V
            e0c    C2                 Ethernet1/1/2    N3K-C3132Q-V
            e0d    C1                 Ethernet1/1/2    N3K-C3132Q-V
n2         /cdp
            e0a    C1                 Ethernet1/1/3    N3K-C3132Q-V
            e0b    C2                 Ethernet1/1/3    N3K-C3132Q-V
            e0c    C2                 Ethernet1/1/4    N3K-C3132Q-V
            e0d    C1                 Ethernet1/1/4    N3K-C3132Q-V
n3         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3132Q-V
            e4e    C2                 Ethernet1/7      N3K-C3132Q-V
n4         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3132Q-V
            e4e    C2                 Ethernet1/8      N3K-C3132Q-V
12 entries were displayed.
```

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

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

```
Node: n2

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

Node: n3

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

Node: n4

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

```
12 entries were displayed.
```

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

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

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                          cluster-network   10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

CL2                          cluster-network   10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP
C2                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000003
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

3 entries were displayed.
```

2. Remove the replaced Nexus 3132Q-V switch, if it is not already removed automatically:

`system cluster-switch delete`

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

3. Verify that the proper cluster switches are monitored:

```
system cluster-switch show
```

Show example

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

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                          cluster-network    10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network     10.10.1.103
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

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:
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.

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 Cisco Nexus 3132Q-V 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.

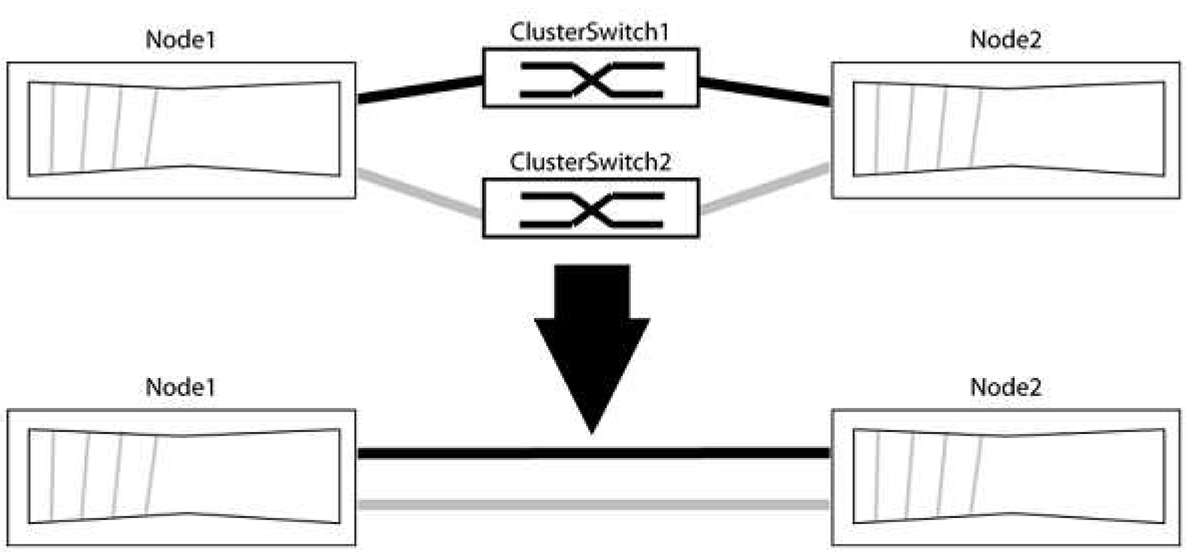
What you'll need

- 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

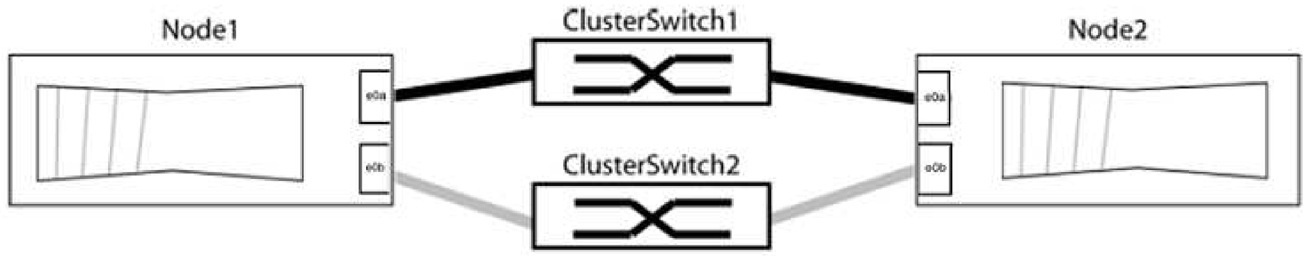
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

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
```

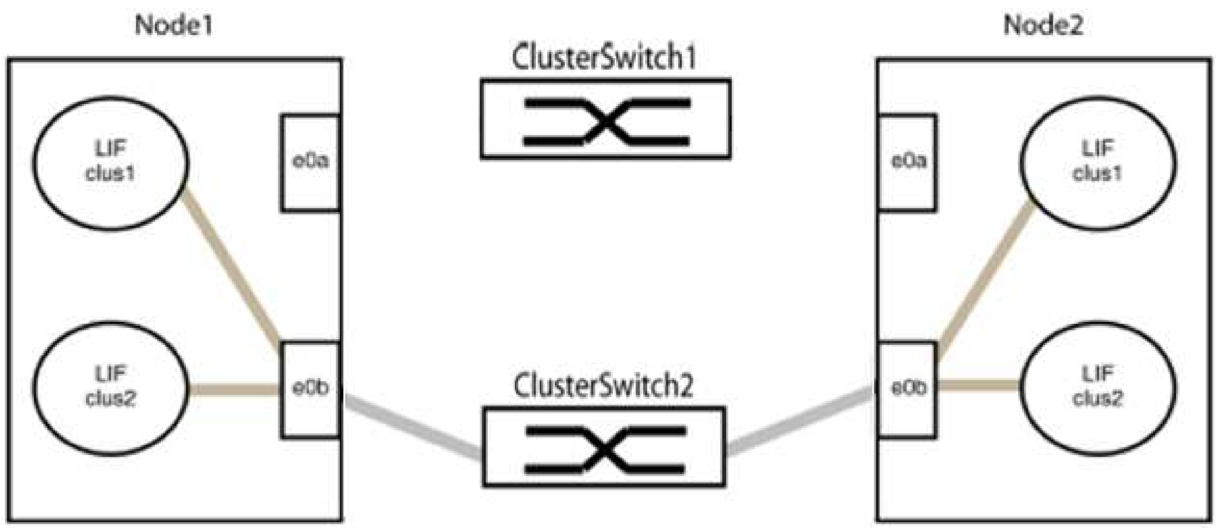
All units must be either master or secondary.

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**.

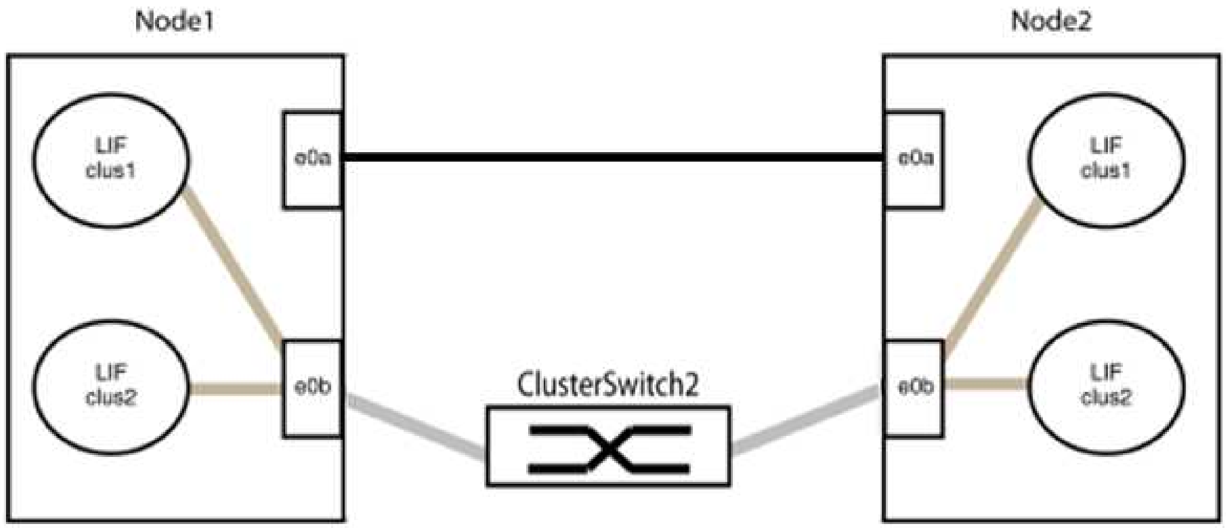
a. Disconnect all the cables from the ports in group1 at the same time.

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:



9. The switchless cluster network option transitions from `false` to `true`. This might take up to 45 seconds. Confirm that the switchless option is set to `true`:

   `network options switchless-cluster show`

   The following example shows that the switchless cluster is enabled:

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

10. Verify that the cluster network is not disrupted:

    `cluster ping-cluster -node local`

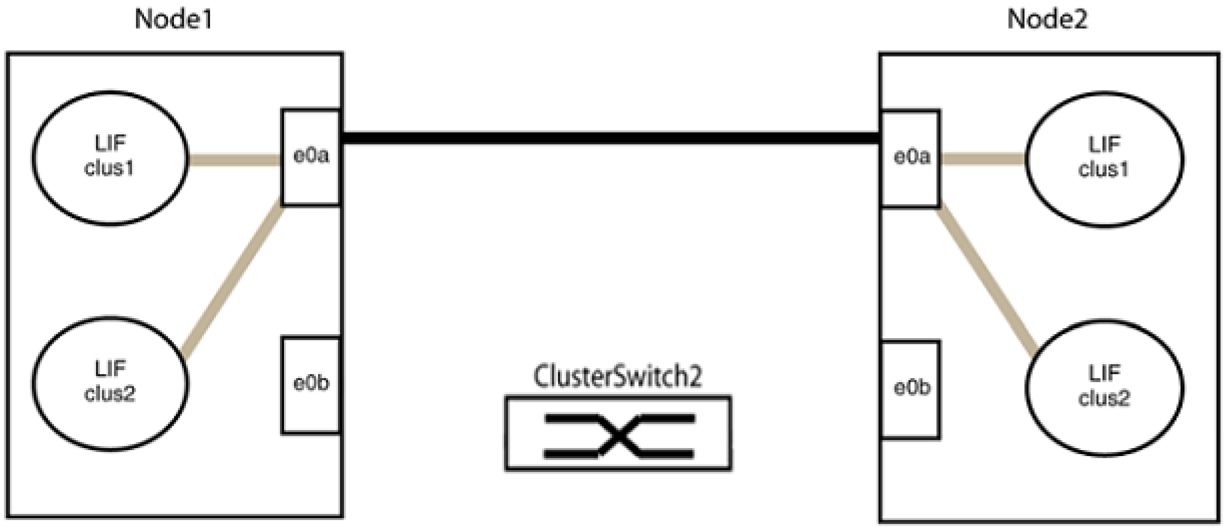
    > Before proceeding to the next step, you must wait at least two minutes to confirm a working back-to-back connection on group 1.

11. Set up the switchless configuration for the ports in group 2.

    > To avoid potential networking issues, you must disconnect the ports from group2 and reconnect them back-to-back as quickly as possible, for example, **in less than 20 seconds**.

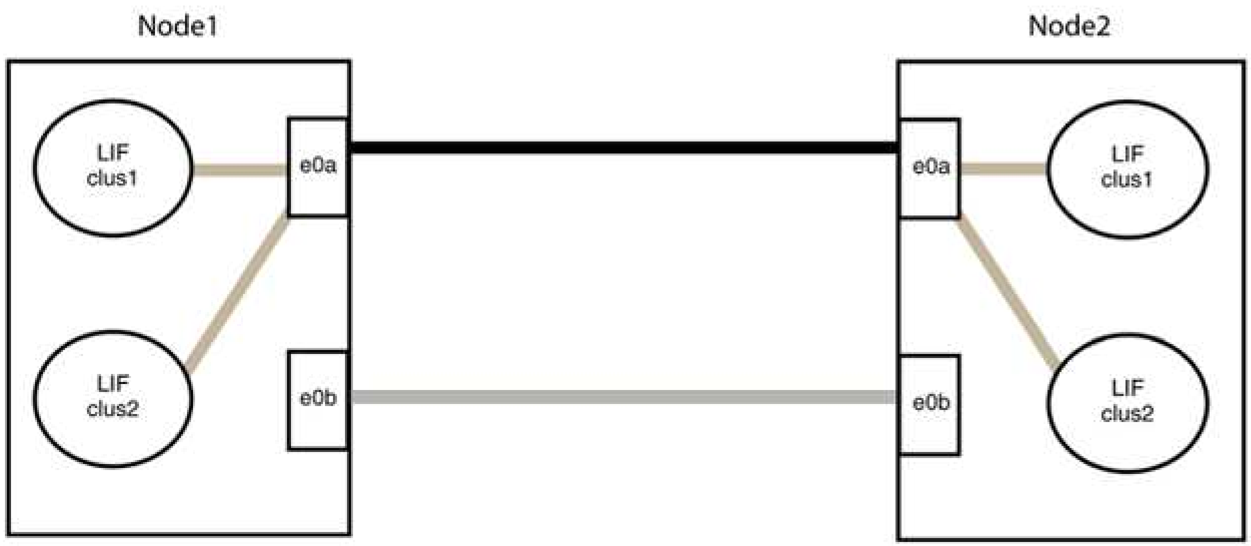
    a. Disconnect all the cables from the ports in group2 at the same time.

       In the following example, the cables are disconnected from port "e0b" on each node, and cluster traffic continues through the direct connection between the "e0a" ports:



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

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



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
```

Cisco Nexus 92300YC

Overview

Overview of installation and configuration for Cisco Nexus 92300YC switches

Before configuring Cisco Nexus 92300YC switches, review the procedure overview.

To initially configure a Cisco Nexus 92300YC switch on systems running ONTAP, follow these steps:

1. Complete Cisco Nexus 92300YC 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. Configure the Cisco Nexus 92300YC switch. Set up and configure the Cisco Nexus 92300YC switch.
3. Prepare to install NX-OS software and Reference Configuration File (RCF). Prepare for installing the NX-OS software and the Reference Configuration File (RCF).
4. Install the NX-OS software. Install the NX-OS software on the Nexus 92300YC switch. NX-OS is a network operating system for the Nexus series of Ethernet switches and MDS series of Fibre Channel (FC) storage area network switches provided by Cisco Systems.
5. Install the Reference Configuration File (RCF). Install the RCF after setting up the Nexus 92300YC switch for the first time. You can also use this procedure to upgrade your RCF version.
6. Install the Cluster Switch Health Monitor (CSHM) configuration file. Install the applicable configuration file for cluster switch health monitoring of Nexus 92300YC cluster switches.

Additional information

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

- Configuration requirements
- Components and part numbers
- Required documentation
- Smart Call Home requirements

Configuration requirements for Cisco Nexus 92300YC switches

For Cisco Nexus 92300YC switch installation and maintenance, be sure to review all configuration and network requirements.

If you want to build ONTAP clusters with more than two nodes, you need two supported cluster network switches. You can use additional management switches, which are optional.

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.

Components for Cisco Nexus 92300YC switches

For Cisco Nexus 92300YC switch installation and maintenance, be sure to review all switch components and part numbers. See the Hardware Universe for details.

The following table lists the part number and description for the 92300YC switch, fans, and power supplies:

Part number	Description
190003	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PTSX (PTSX = Port Side Exhaust)
190003R	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PSIN (PSIN = Port Side Intake)
X-NXA-FAN-35CFM-B	Fan, Cisco N9K port side intake airflow
X-NXA-FAN-35CFM-F	Fan, Cisco N9K port side exhaust airflow
X-NXA-PAC-650W-B	Power supply, Cisco 650W - port side intake
X-NXA-PAC-650W-F	Power supply, Cisco 650W - port side exhaust

Cisco Nexus 92300YC switch airflow details:

- Port-side exhaust airflow (standard air) — Cool air enters the chassis through the fan and power supply modules in the cold aisle and exhausts through the port end of the chassis in the hot aisle. Port-side exhaust airflow with blue coloring.
- Port-side intake airflow (reverse air) — Cool air enters the chassis through the port end in the cold aisle and exhausts through the fan and power supply modules in the hot aisle. Port-side intake airflow with burgundy coloring.

Documentation requirements for Cisco Nexus 92300YC switches

For Cisco Nexus 92300YC switch installation and maintenance, be sure to review all the recommended documentation.

Switch documentation

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

Document title	Description
Nexus 9000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 9000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 9000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 9000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 9000 switches.
Nexus 9000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 9000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 9000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 9000 Series.
Regulatory Compliance and Safety Information for Cisco Nexus 9000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 9000 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 *Installation and Setup Instructions*	Describes how to install NetApp hardware.

Name	Description
ONTAP documentation	Provides detailed information about all aspects of the ONTAP releases.
Hardware Universe	Provides NetApp hardware configuration and compatibility information.

Rail kit and cabinet documentation

To install a Cisco Nexus 92300YC switch in a NetApp cabinet, see the following hardware documentation.

Name	Description
42U System Cabinet, Deep Guide	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.
[Install a Cisco Nexus 92300YC switch in a NetApp Cabinet	Describes how to install a Cisco Nexus 92300YC 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 92300YC 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.

Sample cabling worksheet

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

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	10/25 GbE node	1	10/25 GbE node
2	10/25 GbE node	2	10/25 GbE node
3	10/25 GbE node	3	10/25 GbE node
4	10/25 GbE node	4	10/25 GbE node
5	10/25 GbE node	5	10/25 GbE node
6	10/25 GbE node	6	10/25 GbE node
7	10/25 GbE node	7	10/25 GbE node
8	10/25 GbE node	8	10/25 GbE node
9	10/25 GbE node	9	10/25 GbE node
10	10/25 GbE node	10	10/25 GbE node
11	10/25 GbE node	11	10/25 GbE node
12	10/25 GbE node	12	10/25 GbE node
13	10/25 GbE node	13	10/25 GbE node
14	10/25 GbE node	14	10/25 GbE node
15	10/25 GbE node	15	10/25 GbE node
16	10/25 GbE node	16	10/25 GbE node
17	10/25 GbE node	17	10/25 GbE node
18	10/25 GbE node	18	10/25 GbE node
19	10/25 GbE node	19	10/25 GbE node
20	10/25 GbE node	20	10/25 GbE node

Cluster switch A		Cluster switch B	
21	10/25 GbE node	21	10/25 GbE node
22	10/25 GbE node	22	10/25 GbE node
23	10/25 GbE node	23	10/25 GbE node
24	10/25 GbE node	24	10/25 GbE node
25	10/25 GbE node	25	10/25 GbE node
26	10/25 GbE node	26	10/25 GbE node
27	10/25 GbE node	27	10/25 GbE node
28	10/25 GbE node	28	10/25 GbE node
29	10/25 GbE node	29	10/25 GbE node
30	10/25 GbE node	30	10/25 GbE node
31	10/25 GbE node	31	10/25 GbE node
32	10/25 GbE node	32	10/25 GbE node
33	10/25 GbE node	33	10/25 GbE node
34	10/25 GbE node	34	10/25 GbE node
35	10/25 GbE node	35	10/25 GbE node
36	10/25 GbE node	36	10/25 GbE node
37	10/25 GbE node	37	10/25 GbE node
38	10/25 GbE node	38	10/25 GbE node
39	10/25 GbE node	39	10/25 GbE node
40	10/25 GbE node	40	10/25 GbE node
41	10/25 GbE node	41	10/25 GbE node
42	10/25 GbE node	42	10/25 GbE node

Cluster switch A		Cluster switch B	
43	10/25 GbE node	43	10/25 GbE node
44	10/25 GbE node	44	10/25 GbE node
45	10/25 GbE node	45	10/25 GbE node
46	10/25 GbE node	46	10/25 GbE node
47	10/25 GbE node	47	10/25 GbE node
48	10/25 GbE node	48	10/25 GbE node
49	40/100 GbE node	49	40/100 GbE node
50	40/100 GbE node	50	40/100 GbE node
51	40/100 GbE node	51	40/100 GbE node
52	40/100 GbE node	52	40/100 GbE node
53	40/100 GbE node	53	40/100 GbE node
54	40/100 GbE node	54	40/100 GbE node
55	40/100 GbE node	55	40/100 GbE node
56	40/100 GbE node	56	40/100 GbE node
57	40/100 GbE node	57	40/100 GbE node
58	40/100 GbE node	58	40/100 GbE node
59	40/100 GbE node	59	40/100 GbE node
60	40/100 GbE node	60	40/100 GbE node
61	40/100 GbE node	61	40/100 GbE node
62	40/100 GbE node	62	40/100 GbE node
63	40/100 GbE node	63	40/100 GbE node
64	40/100 GbE node	64	40/100 GbE node

Cluster switch A		Cluster switch B	
65	100 GbE ISL to switch B port 65	65	100 GbE ISL to switch A port 65
66	100 GbE ISL to switch B port 66	66	100 GbE ISL to switch A port 65

Blank cabling worksheet

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

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

Cluster switch A		Cluster switch B	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	
37		37	

Cluster switch A		Cluster switch B	
38		38	
39		39	
40		40	
41		41	
42		42	
43		43	
44		44	
45		45	
46		46	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	

Cluster switch A		Cluster switch B	
60		60	
61		61	
62		62	
63		63	
64		64	
65	ISL to switch B port 65	65	ISL to switch A port 65
66	ISL to switch B port 66	66	ISL to switch A port 66

Configure the Cisco Nexus 92300YC switch

Follow this procedure to set up and configure the Cisco Nexus 92300YC switch.

Steps

1. Connect the serial port to a host or serial port.
2. Connect the management port (on the non-port side of the switch) to the same network where your SFTP server is located.
3. At the console, set the host side serial settings:
   - 9600 baud
   - 8 data bits
   - 1 stop bit
   - parity: none
   - flow control: none
4. When booting for the first time or rebooting after erasing the running configuration, the Nexus 92300YC switch loops in a boot cycle. Interrupt this cycle by typing **yes** to abort Power on Auto Provisioning.

   The System Admin Account setup is displayed.

Show example

```
$ VDC-1 %$ %POAP-2-POAP_INFO:   - Abort Power On Auto Provisioning
[yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning]
(yes/skip/no)[no]: y
Disabling POAP.......Disabling POAP
2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please
wait... (This may take 5-15 minutes)

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

Do you want to enforce secure password standard (yes/no) [y]:
```

5. Type **y** to enforce secure password standard:

```
Do you want to enforce secure password standard (yes/no) [y]: y
```

6. Enter and confirm the password for user admin:

```
Enter the password for "admin":
Confirm the password for "admin":
```

7. Type **yes** to enter the Basic System Configuration dialog.

Show example

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

Please register Cisco Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 devices must be registered to receive
entitled support services.

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

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

8. Create another login account:

```
Create another login account (yes/no) [n]:
```

9. Configure read-only and read-write SNMP community strings:

```
Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:
```

10. Configure the cluster switch name:

```
Enter the switch name : cs2
```

11. Configure the out-of-band management interface:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address : 172.22.133.216

Mgmt0 IPv4 netmask : 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : 172.22.128.1
```

12. Configure advanced IP options:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Configure Telnet services:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Configure SSH services and SSH keys:

```
Enable the ssh service? (yes/no) [y]: y

       Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa

       Number of rsa key bits <1024-2048> [1024]: 2048
```

15. Configure other settings:

```
Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L2]: L2

  Configure default switchport interface state (shut/noshut) [noshut]:
noshut

  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: strict
```

16. Confirm switch information and save the configuration:

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

Use this configuration and save it? (yes/no) [y]: y

[] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

What's next?

Prepare to install NX-OS software and RCF.

Review cabling and configuration considerations

Before configuring your Cisco 92300YC 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.

What you'll need

- A fully functioning cluster (no errors in the logs or similar issues).
- Appropriate software and upgrade guides, which are available from Cisco Nexus 9000 Series Switches.

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

- The names of the two Cisco switches are `cs1` and `cs2`.
- The node names are `node1` and `node2`.
- The cluster LIF names are `node1_clus1` and `node1_clus2` for node1 and `node2_clus1` and `node2_clus2` for node2.
- The `cluster1::*>` prompt indicates the name of the cluster.

About this task

The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated. The command outputs might vary depending on different releases of ONTAP.

Steps

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

   ```
   set -privilege advanced
   ```

   The advanced prompt (`*>`) appears.

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

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

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

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

   The following command suppresses automatic case creation for two hours:

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

3. 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/       Local  Discovered
   Protocol     Port   Device (LLDP: ChassisID)  Interface
   Platform
   ----------- ------ ------------------------- ----------------
   ----------------
   node2      /cdp
               e0a    cs1                       Eth1/2            N9K-
   C92300YC
               e0b    cs2                       Eth1/2            N9K-
   C92300YC
   node1      /cdp
               e0a    cs1                       Eth1/1            N9K-
   C92300YC
               e0b    cs2                       Eth1/1            N9K-
   C92300YC

   4 entries were displayed.
   ```

4. Check the administrative or operational status of each cluster interface.

   a. Display the network port attributes: `network port show -ipspace Cluster`

Show example

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

Node: node2
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: node1
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. Display information about the LIFs: `network interface show -vserver Cluster`

Show example

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

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.
```

5. Ping the remote cluster LIFs:

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

Show example

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

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

```
network interface show -vserver Cluster -fields auto-revert
```

Show example

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

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

4 entries were displayed.
```

7. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files using the commands:

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

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.

What's next?

Install the NX-OS software.

Install the NX-OS software

Follow this procedure to install the NX-OS software on the Nexus 92300YC switch.

NX-OS is a network operating system for the Nexus series of Ethernet switches and MDS series of Fibre Channel (FC) storage area network switches provided by Cisco Systems.

Review requirements

Supported ports and node connections

- The Inter-Switch Links (ISLs) supported for the Nexus 92300YC switches are ports 1/65 and 1/66.
- The node connections supported for the Nexus 92300YC switches are ports 1/1 through 1/66.

What you'll need

- Applicable NetApp Cisco NX-OS software for your switches from the NetApp Support Site, available from mysupport.netapp.com
- 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.

Install the software

The examples in this procedure use two nodes, but you can have up to 24 nodes in a cluster.

About the examples

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

- The Nexus 92300YC switch names are `cs1` and `cs2`.
- The example used in this procedure starts the upgrade on the second switch, **cs2*.*
- The cluster LIF names are `node1_clus1` and `node1_clus2` for node1, and `node2_clus1` and `node2_clus2` for node2.
- The IPspace name is `Cluster`.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The cluster ports on each node are named `e0a` and `e0b`.

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

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 92300YC switch.

Show example

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.2.2.bin  /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.2.2.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.2.2.img  /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

```
show version
```

Show example

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.31
  NXOS: version 9.2(1)
  BIOS compile time:  05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time:  7/17/2018 16:00:00 [07/18/2018 00:21:19]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
  System version: 9.2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

5. Install the NX-OS image.

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

Show example

```
cs2# install all nxos bootflash:nxos.9.2.2.bin

Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS

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

Notifying services about system upgrade.
[] 100% -- SUCCESS



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



Images will be upgraded according to following table:

Module   Image         Running-Version(pri:alt            New-
Version         Upg-Required
------  --------  --------------------------------------
-------------------  ------------
  1       nxos                                9.2(1)
9.2(2)         yes
  1       bios    v05.31(05/17/2018):v05.28(01/18/2018)
v05.33(09/08/2018)       yes
```

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


Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading
bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[] 100% -- SUCCESS
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully deactivated virtual service 'guestshell+'

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

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

```
show version
```

Show example

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.33
  NXOS: version 9.2(2)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.2.2.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]



Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)

Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```

```
  Reason: Reset due to upgrade
  System version: 9.2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

7. Upgrade the EPLD image and reboot the switch.

Show example

```
cs2# show version module 1 epld

EPLD Device                     Version
---------------------------------------
MI  FPGA                         0x7
IO  FPGA                         0x17
MI  FPGA2                        0x2
GEM FPGA                         0x2
GEM FPGA                         0x2
GEM FPGA                         0x2
GEM FPGA                         0x2

cs2# install epld bootflash:n9000-epld.9.2.2.img module 1
Compatibility check:
Module        Type         Upgradable        Impact   Reason
------  -----------------  ----------    ----------   ------
     1            SUP           Yes       disruptive  Module
Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------  ----  -------------      ---------------   -----------
------------
     1   SUP  MI FPGA                   0x07        0x07
No
     1   SUP  IO FPGA                   0x17        0x19
Yes
     1   SUP  MI FPGA2                  0x02        0x02
No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64
sectors)
Module 1 EPLD upgrade is successful.
Module        Type  Upgrade-Result
------  ------------------  --------------
```

```
     1          SUP          Success


EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

8. After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

   Show example

   ```
   cs2# *show version module 1 epld*

   EPLD Device                         Version
   ---------------------------------------
   MI  FPGA                             0x7
   IO  FPGA                             0x19
   MI  FPGA2                            0x2
   GEM FPGA                             0x2
   GEM FPGA                             0x2
   GEM FPGA                             0x2
   GEM FPGA                             0x2
   ```

What's next?

Install the Reference Configuration File

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 92300YC switch for the first time. You can also use this procedure to upgrade your RCF version.

About this task

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

- The names of the two Cisco switches are `cs1` and `cs2`.
- The node names are `node1` and `node2`.
- The cluster LIF names are `node1_clus1`, `node1_clus2`, `node2_clus1`, and `node2_clus2`.
- The `cluster1::*>` prompt indicates the name of the cluster.

- The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches; ONTAP commands are used unless otherwise indicated.
- Before you perform this procedure, make sure that you have a current backup of the switch configuration.
- 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.

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
----------- ------ ------------------------- ----------------
------------
node1/cdp
             e0a    cs1                       Ethernet1/1/1     N9K-
C92300YC
             e0b    cs2                       Ethernet1/1/1     N9K-
C92300YC
node2/cdp
             e0a    cs1                       Ethernet1/1/2     N9K-
C92300YC
             e0b    cs2                       Ethernet1/1/2     N9K-
C92300YC
cluster1::*>
```

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

Show example

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

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
cluster1::*>
```

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

Show example

```
cluster1::*> *network interface show -vserver Cluster*
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            node1_clus1        up/up      169.254.3.4/23    node1
e0c     true
            node1_clus2        up/up      169.254.3.5/23    node1
e0d     true
            node2_clus1        up/up      169.254.3.8/23    node2
e0c     true
            node2_clus2        up/up      169.254.3.9/23    node2
e0d     true
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
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.93
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

3. Disable auto-revert on the cluster LIFs.

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

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

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. Verify that the cluster ports have migrated to the ports hosted on cluster switch cs1. This might take a few seconds. `network interface show -vserver Cluster`

Show example

```
cluster1::*> *network interface show -vserver Cluster*
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1       up/up      169.254.3.4/23     node1
e0c     true
            node1_clus2       up/up      169.254.3.5/23     node1
e0c     false
            node2_clus1       up/up      169.254.3.8/23     node2
e0c     true
            node2_clus2       up/up      169.254.3.9/23     node2
e0c     false
cluster1::*>
```

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

Show example

```
cluster1::*> *cluster show*
Node           Health  Eligibility   Epsilon
-------------- ------- ------------  -------
node1          true    true          false
node2          true    true          false
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 perform a basic setup.

> When updating or applying a new RCF, you must erase the switch settings and perform basic configuration. You must be connected to the switch 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. Perform a reboot of the switch:

Show example

```
(cs2)# reload

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

9. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series Switches guides.

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

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: /code/Nexus_92300YC_RCF_v1.0.2.txt
Enter hostname for the tftp 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:
tftp> progress
Progress meter enabled
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin
/code/Nexus_92300YC_R  100% 9687   530.2KB/s   00:00
tftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

10. Apply the RCF previously downloaded to the bootflash.

    For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series Switches guides.

This example shows the RCF file `Nexus_92300YC_RCF_v1.0.2.txt` being installed on switch cs2:

```
cs2# copy Nexus_92300YC_RCF_v1.0.2.txt running-config echo-commands

Disabling ssh: as its enabled right now:
 generating ecdsa key(521 bits)......
generated ecdsa key

Enabling ssh: as it has been disabled
 this command enables edge port type (portfast) by default on all
interfaces. You
 should now disable edge port type (portfast) explicitly on switched
ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.

Edge port type (portfast) should only be enabled on ports connected to a
single
 host. Connecting hubs, concentrators, switches, bridges, etc...  to
this
 interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
 Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet1/1 but will
only
 have effect when the interface is in a non-trunking mode.

...

Copy complete, now saving to disk (please wait)...
Copy complete.
```

11. Verify on the switch that the RCF has been merged successfully:

    `show running-config`

```
cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019

version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJ1RtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #

*
*
*  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
*
*
*
*  Ports 1/1  - 1/48: 10GbE Intra-Cluster Node Ports
*
*  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
*
*  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
*
*
*
```

ⓘ When applying the RCF for the first time, the **ERROR: Failed to write VSH commands** message is expected and can be ignored.

12. Verify that the RCF file is the correct newer version: `show running-config`

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

- The RCF banner
- The node and port settings
- Customizations

  The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.

13. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file.

    For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series Switches guides.

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

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

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

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

    a. Verify that e0d ports are up and healthy across all nodes in the cluster: `network port show -ipspace Cluster`

Show example

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

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

b. Verify 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
----------- ------ ------------------------- -----------------
------------
node1/cdp
            e0a    cs1                       Ethernet1/1
N9K-C92300YC
            e0b    cs2                       Ethernet1/1
N9K-C92300YC
node2/cdp
            e0a    cs1                       Ethernet1/2
N9K-C92300YC
            e0b    cs2                       Ethernet1/2
N9K-C92300YC

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
------------
cs1                         cluster-network    10.233.205.90
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

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

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

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

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

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

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

    Show example

```
cluster1::*> *network interface show -vserver Cluster*
            Logical          Status     Network            Current
Current Is
Vserver     Interface        Admin/Oper Address/Mask       Node
Port    Home
----------- ---------------- ---------- ------------------
----------------- ------- ----
Cluster
            node1_clus1      up/up      169.254.3.4/23     node1
e0d     false
            node1_clus2      up/up      169.254.3.5/23     node1
e0d     true
            node2_clus1      up/up      169.254.3.8/23     node2
e0d     false
            node2_clus2      up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

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

Show example

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

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

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

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

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

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

```
cs1# show interface brief | grep up
.
.
Ethernet1/1      1       eth  access up      none
10G(D) --
Ethernet1/2      1       eth  access up      none
10G(D) --
Ethernet1/3      1       eth  trunk  up      none
100G(D) --
Ethernet1/4      1       eth  trunk  up      none
100G(D) --
.
.
```

23. 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      Eth1/65(P)   Eth1/66(P)
cs1#
```

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

Show example

```
cluster1::*> *network interface show -vserver Cluster*
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1   up/up      169.254.3.4/23     node1
e0d     true
            node1_clus2   up/up      169.254.3.5/23     node1
e0d     true
            node2_clus1   up/up      169.254.3.8/23     node2
e0d     true
            node2_clus2   up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

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

Show example

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

26. Ping the remote cluster interfaces to verify connectivity: `cluster ping-cluster -node local`

Show example

```
cluster1::*> *cluster ping-cluster -node local*
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 e0b
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)
```

For ONTAP 9.8 and later

For ONTAP 9.8 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands: `system switch ethernet log setup-password` and `system switch ethernet log enable-collection`

Enter: `system switch ethernet log setup-password`

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

Followed by: `system switch ethernet log enable-collection`

```
cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```

For ONTAP 9.4 and later

For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files using the commands:

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

Enter: `system cluster-switch log setup-password`

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

Followed by: `system cluster-switch log enable-collection`

```
cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```

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

Ethernet Switch Health Monitoring log collection

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.

Steps

1. To set up log collection, run the following command for each switch. You are prompted to enter the switch name, username, and password for log collection.

   `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.

Troubleshoot

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

switch dump log error	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 92300YC 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: cshm1!
                                  Model Number: N9K-C92300YC
                                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: N9K-C92300YC
                                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

Migrate to a two-node switched cluster with a Cisco Nexus 92300YC switch

If you have an existing two-node *switchless* cluster environment, you can migrate to a two-node *switched* cluster environment using Cisco Nexus 92300YC switches to enable you to scale beyond two nodes in the cluster.

The procedure you use depends on whether you have two dedicated cluster-network ports on each controller or a single cluster port on each controller. The process documented works for all nodes using optical or twinax ports, but is not supported on this switch if nodes are using onboard 10Gb BASE-T RJ45 ports for the cluster-network ports.

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

> After your migration completes, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for 92300YC cluster switches. See Install the Cluster Switch Health Monitor (CSHM).

Review requirements

What you'll need

For a two-node switchless configuration, ensure that:

- The two-node switchless configuration is properly set up and functioning.
- The nodes are running ONTAP 9.6 and later.
- All cluster ports are in the **up** state.
- All cluster logical interfaces (LIFs) are in the **up** state and on their home ports.

For the Cisco Nexus 92300YC switch configuration:

- Both switches have management network connectivity.
- There is console access to the cluster switches.
- Nexus 92300YC node-to-node switch and switch-to-switch connections use twinax or fiber cables.

  Hardware Universe - Switches contains more information about cabling.

- Inter-Switch Link (ISL) cables are connected to ports 1/65 and 1/66 on both 92300YC switches.
- Initial customization of both the 92300YC switches are completed. So that the:
  - 92300YC switches are running the latest version of software
  - Reference Configuration Files (RCFs) are applied to the switches Any site customization, such as SMTP, SNMP, and SSH is configured on the new switches.

Migrate the switch

About the examples

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

- The names of the 92300YC switches are cs1 and cs2.
- The names of the cluster SVMs are node1 and node2.
- The names of the LIFs are node1_clus1 and node1_clus2 on node 1, and node2_clus1 and node2_clus2 on node 2 respectively.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The cluster ports used in this procedure are e0a and e0b.

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

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

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

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

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

Show example

The following command suppresses automatic case creation for two hours:

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

Step 2: Configure cables and ports

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

   You must not disable the ISL ports.

   Show example

   The following example shows that node-facing ports 1 through 64 are disabled on switch cs1:

   ```
   cs1# config
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e/1-64
   cs1(config-if-range)# shutdown
   ```

2. Verify that the ISL and the physical ports on the ISL between the two 92300YC switches cs1 and cs2 are up on ports 1/65 and 1/66:

   ```
   show port-channel summary
   ```

Show example

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

```
cs1# show port-channel summary

Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        b - BFD Session Wait
        S - Switched     R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
```

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

+

```
(cs2)# show port-channel summary

Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        b - BFD Session Wait
        S - Switched     R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
```

3. Display the list of neighboring devices:

   ```
   show cdp neighbors
   ```

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

Show example

The following example lists the neighboring devices on switch cs1:

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

+ The following example lists the neighboring devices on switch cs2:

+

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs1(FDO220329KU)    Eth1/65        177    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)    Eth1/66        177    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

4. Verify that all cluster ports are up:

`network port show -ipspace Cluster`

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

Show example

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

Node: node1

                                                       Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper  Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: node2

                                                       Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper  Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

5. Verify that all cluster LIFs are up and operational:

   `network interface show -vserver Cluster`

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

Show example

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

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
4 entries were displayed.
```

6. Verify that auto-revert 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

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

4 entries were displayed.
```

7. Disconnect the cable from cluster port e0a on node1, and then connect e0a to port 1 on cluster switch cs1, using the appropriate cabling supported by the 92300YC switches.

The *Hardware Universe - Switches* contains more information about cabling.

8. Disconnect the cable from cluster port e0a on node2, and then connect e0a to port 2 on cluster switch cs1, using the appropriate cabling supported by the 92300YC switches.
9. Enable all node-facing ports on cluster switch cs1.

Show example

The following example shows that ports 1/1 through 1/64 are enabled on switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-64
cs1(config-if-range)# no shutdown
```

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

`network interface show -vserver Cluster`

Show example

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

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

          Logical       Status     Network            Current
Current Is
Vserver  Interface     Admin/Oper Address/Mask       Node          Port
Home
-------- ------------ ---------- ------------------ -----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1         e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1         e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2         e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2         e0b
true

4 entries were displayed.
```

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

    `cluster show`

    Show example

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

```
cluster1::*> cluster show

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

2 entries were displayed.
```

12. Disconnect the cable from cluster port e0b on node1, and then connect e0b to port 1 on cluster switch cs2, using the appropriate cabling supported by the 92300YC switches.
13. Disconnect the cable from cluster port e0b on node2, and then connect e0b to port 2 on cluster switch cs2, using the appropriate cabling supported by the 92300YC switches.
14. Enable all node-facing ports on cluster switch cs2.

    Show example

    The following example shows that ports 1/1 through 1/64 are enabled on switch cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-64
cs2(config-if-range)# no shutdown
```

Step 3: Verify the configuration

1. Verify that all cluster ports are up:

    `network port show -ipspace Cluster`

Show example

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

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

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

4 entries were displayed.
```

2. Verify that all interfaces display true for `Is Home`:

   `network interface show -vserver Cluster`

   > This might take several minutes to complete.

Show example

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

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

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node        Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1       e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1       e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2       e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2       e0b
true

4 entries were displayed.
```

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

`show cdp neighbors`

Show example

The following example shows the appropriate results for both switches:

```
(cs1)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         133    H         FAS2980
e0a
node2               Eth1/2         133    H         FAS2980
e0a
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4


(cs2)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         133    H         FAS2980
e0b
node2               Eth1/2         133    H         FAS2980
e0b
cs1(FDO220329KU)
                    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

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

   `network device-discovery show -protocol cdp`

   Show example

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2              N9K-
C92300YC
            e0b    cs2                       0/2              N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1              N9K-
C92300YC
            e0b    cs2                       0/1              N9K-
C92300YC

4 entries were displayed.
```

5. Verify that the settings are disabled:

   `network options switchless-cluster show`

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

   Show example

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

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

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

   `cluster show`

Show example

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

```
cluster1::*> cluster show

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

7. Verify that the cluster network has full connectivity:

   `cluster ping-cluster -node node-name`

   Show example

```
cluster1::> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

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

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

Show example

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

9. Change the privilege level back to admin:

   `set -privilege admin`

10. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands:

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

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.

Migrate from a Cisco switch to a Cisco Nexus 92300YC switch

You can migrate nondisruptively older Cisco cluster switches for an ONTAP cluster to

Cisco Nexus 92300YC cluster network switches.

> After your migration completes, you might need to install the required configuration file to support the Cluster Switch Health Monitor (CSHM) for 92300YC cluster switches. See Install the Cluster Switch Health Monitor (CSHM).

Review requirements

What you'll need

- A fully functional existing cluster.
- 10 GbE and 40 GbE connectivity from nodes to Nexus 92300YC cluster switches.
- All cluster ports are in the up state to ensure nondisruptive operations.
- Proper version of NX-OS and reference configuration file (RCF) installed on the Nexus 92300YC cluster switches.
- A redundant and fully functional NetApp cluster using both older Cisco switches.
- Management connectivity and console access to both the older Cisco switches and the new switches.
- All cluster LIFs in the up state with the cluster LIFs are on their home ports.
- ISL ports enabled and cabled between the older Cisco switches and between the new switches.

Migrate the switch

About the examples

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

- The existing Cisco Nexus 5596UP cluster switches are c1 and c2.
- The new Nexus 92300YC cluster switches are cs1 and cs2.
- The nodes are node1 and node2.
- The cluster LIFs are node1_clus1 and node1_clus2 on node 1, and node2_clus1 and node2_clus2 on node 2 respectively.
- Switch c2 is replaced by switch cs2 first and then switch c1 is replaced by switch cs1.
    - A temporary ISL is built on cs1 connecting c1 to cs1.
    - Cabling between the nodes and c2 are then disconnected from c2 and reconnected to cs2.
    - Cabling between the nodes and c1 are then disconnected from c1 and reconnected to cs1.
    - The temporary ISL between c1 and cs1 is then removed.

Ports used for connections

- Some of the ports are configured on Nexus 92300YC switches to run at 10 GbE or 40 GbE.
- The cluster switches use the following ports for connections to nodes:
    - Ports e1/1-48 (10/25 GbE), e1/49-64 (40/100 GbE): Nexus 92300YC
    - Ports e1/1-40 (10 GbE): Nexus 5596UP
    - Ports e1/1-32 (10 GbE): Nexus 5020
    - Ports e1/1-12, e2/1-6 (10 GbE): Nexus 5010 with expansion module
- The cluster switches use the following Inter-Switch Link (ISL) ports:

    - Ports e1/65-66 (100 GbE): Nexus 92300YC
    - Ports e1/41-48 (10 GbE): Nexus 5596UP
    - Ports e1/33-40 (10 GbE): Nexus 5020
    - Ports e1/13-20 (10 GbE): Nexus 5010
- Hardware Universe - Switches contains information about supported cabling for all cluster switches.
- The ONTAP and NX-OS versions supported in this procedure are on the Cisco Ethernet Switches page.

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

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

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

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

   Show example

   The following command suppresses automatic case creation for two hours:

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

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

   `network interface show -vserver Cluster -fields auto-revert`

Show example

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

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

4 entries were displayed.
```

4. Determine the administrative or operational status for each cluster interface:

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

   a. Display the network port attributes:

      `network port show -ipspace Cluster`

Show example

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

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

4 entries were displayed.
```

b. Display information about the logical interfaces and their designated home nodes:

`network interface show -vserver Cluster`

Each LIF should display up/up for `Status Admin/Oper` and true for `Is Home`.

Show example

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true

4 entries were displayed.
```

5. Verify that the cluster ports on each node are connected to existing cluster switches in the following way (from the nodes' perspective) using the command:

   `network device-discovery show -protocol cdp`

Show example

```
cluster1::*> network device-discovery show -protocol cdp
Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
             e0a    c1                        0/2              N5K-
C5596UP
             e0b    c2                        0/2              N5K-
C5596UP
node1      /cdp
             e0a    c1                        0/1              N5K-
C5596UP
             e0b    c2                        0/1              N5K-
C5596UP

4 entries were displayed.
```

6. Verify that the cluster ports and switches are connected in the following way (from the switches' perspective) using the command:

   `show cdp neighbors`

Show example

```
c1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0a
node2               Eth1/2         124    H         FAS2750
e0a
c2(FOX2025GEFC)     Eth1/41        179    S I s     N5K-C5596UP
Eth1/41

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

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

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

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

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

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

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

Total entries displayed: 10


c2# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID              Local Intrfce Hldtme Capability  Platform
Port ID
node1                Eth1/1         124    H         FAS2750
e0b
node2                Eth1/2         124    H         FAS2750
e0b
c1(FOX2025GEEX)      Eth1/41        175    S I s     N5K-C5596UP
Eth1/41

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

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

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

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

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

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

c1(FOX2025GEEX)      Eth1/48        176    S I s     N5K-C5596UP
Eth1/48
```

7. Verify that the cluster network has full connectivity using the command:

   `cluster ping-cluster -node node-name`

Show example

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Step 2: Configure cables and ports

1. Configure a temporary ISL on cs1on ports e1/41-48, between c1 and cs1.

Show example

The following example shows how the new ISL is configured on c1 and cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/41-48
cs1(config-if-range)# description temporary ISL between Nexus 5596UP
and Nexus 92300YC
cs1(config-if-range)# no lldp transmit
cs1(config-if-range)# no lldp receive
cs1(config-if-range)# switchport mode trunk
cs1(config-if-range)# no spanning-tree bpduguard enable
cs1(config-if-range)# channel-group 101 mode active
cs1(config-if-range)# exit
cs1(config)# interface port-channel 101
cs1(config-if)# switchport mode trunk
cs1(config-if)# spanning-tree port type network
cs1(config-if)# exit
cs1(config)# exit
```

2. Remove ISL cables from ports e1/41-48 from c2 and connect the cables to ports e1/41-48 on cs1.
3. Verify that the ISL ports and port-channel are operational connecting c1 and cs1:

```
show port-channel summary
```

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 cs1:

```
c1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/41(P)   Eth1/42(P)
Eth1/43(P)
                                     Eth1/44(P)   Eth1/45(P)
Eth1/46(P)
                                     Eth1/47(P)   Eth1/48(P)


cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
101   Po101(SU)   Eth      LACP      Eth1/41(P)   Eth1/42(P)
Eth1/43(P)
                                     Eth1/44(P)   Eth1/45(P)
Eth1/46(P)
                                     Eth1/47(P)   Eth1/48(P)
```

4. For node1, disconnect the cable from e1/1 on c2, and then connect the cable to e1/1 on cs2, using appropriate cabling supported by Nexus 92300YC.
5. For node2, disconnect the cable from e1/2 on c2, and then connect the cable to e1/2 on cs2, using appropriate cabling supported by Nexus 92300YC.
6. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective:

   `network device-discovery show -protocol cdp`

   Show example

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

Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
             e0a    c1                        0/2              N5K-
C5596UP
             e0b    cs2                       0/2              N9K-
C92300YC
node1      /cdp
             e0a    c1                        0/1              N5K-
C5596UP
             e0b    cs2                       0/1              N9K-
C92300YC

4 entries were displayed.
```

7. For node1, disconnect the cable from e1/1 on c1, and then connect the cable to e1/1 on cs1, using appropriate cabling supported by Nexus 92300YC.
8. For node2, disconnect the cable from e1/2 on c1, and then connect the cable to e1/2 on cs1, using appropriate cabling supported by Nexus 92300YC.
9. The cluster ports on each node are now connected to cluster switches in the following way, from the nodes' perspective:

   `network device-discovery show -protocol cdp`

Show example

```
cluster1::*> network device-discovery show -protocol cdp
Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
             e0a    cs1                       0/2              N9K-
C92300YC
             e0b    cs2                       0/2              N9K-
C92300YC
node1      /cdp
             e0a    cs1                       0/1              N9K-
C92300YC
             e0b    cs2                       0/1              N9K-
C92300YC
4 entries were displayed.
```

10. Delete the temporary ISL between cs1 and c1.

Show example

```
cs1(config)# no interface port-channel 10
cs1(config)# interface e1/41-48
cs1(config-if-range)# lldp transmit
cs1(config-if-range)# lldp receive
cs1(config-if-range)# no switchport mode trunk
cs1(config-if-range)# no channel-group
cs1(config-if-range)# description 10GbE Node Port
cs1(config-if-range)# spanning-tree bpduguard enable
cs1(config-if-range)# exit
cs1(config)# exit
```

Step 3: Complete the migration

1. Verify the final configuration of the cluster:

   `network port show -ipspace Cluster`

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

Show example

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

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
```

```
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.


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

Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2              N9K-
C92300YC
            e0b    cs2                       0/2              N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1              N9K-
C92300YC
            e0b    cs2                       0/1              N9K-
C92300YC

4 entries were displayed.


cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0a
node2               Eth1/2         124    H         FAS2750
e0a
cs2(FDO220329V5)    Eth1/65        179    R S I s   N9K-C92300YC
Eth1/65
```

```
cs2(FDO220329V5)    Eth1/66        179    R S I s   N9K-C92300YC
Eth1/66


cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0b
node2               Eth1/2         124    H         FAS2750
e0b
cs1(FDO220329KU)
                    Eth1/65        179    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                    Eth1/66        179    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

2. Verify that the cluster network has full connectivity:

`cluster ping-cluster -node node-name`

Show example

```
cluster1::*> set -priv advanced

Warning: These advanced commands are potentially dangerous; use them
only when
         directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)


cluster1::*> set -privilege admin
cluster1::*>
```

3. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using the commands:

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

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.

Replace switches

Replace a Cisco Nexus 92300YC switch

Replacing a defective Nexus 92300YC switch in a cluster network is a nondisruptive procedure (NDU).

Review requirements

What you'll need

Before performing the switch replacement, ensure that:

- In the existing cluster and network infrastructure:
  - The existing cluster is verified as completely functional, with at least one fully connected cluster switch.
  - All cluster ports are up.
  - All cluster logical interfaces (LIFs) are up and on their home ports.
  - The ONTAP cluster ping-cluster -node node1 command must indicate that basic connectivity and larger than PMTU communication are successful on all paths.
- For the Nexus 92300YC replacement switch:
  - Management network connectivity on the replacement switch are functional.
  - Console access to the replacement switch are in place.
  - The node connections are ports 1/1 through 1/64.
  - All Inter-Switch Link (ISL) ports are disabled on ports 1/65 and 1/66.
  - The desired reference configuration file (RCF) and NX-OS operating system image switch are loaded onto the switch.
  - Initial customization of the switch are complete, as detailed in: Configure the Cisco Nexus 92300YC switch.

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

Replace the switch

About the examples

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

- The names of the existing Nexus 92300YC switches are cs1 and cs2.
- The name of the new Nexus 92300YC switch is newcs2.
- The node names are node1 and node2.
- The cluster ports on each node are named e0a and e0b.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The prompt for changes to all cluster nodes is cluster1::*>

About this task

You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.

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

Show topology

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

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
false
e0b       Cluster      Cluster          up   9000  auto/10000 healthy
false
4 entries were displayed.



cluster1::*> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e0a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e0b
```

```
true
            node2_clus1  up/up    169.254.47.194/16  node2         e0a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e0b
true
4 entries were displayed.



cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2            N9K-
C92300YC
            e0b    cs2                       Eth1/2            N9K-
C92300YC
node1      /cdp
            e0a    cs1                       Eth1/1            N9K-
C92300YC
            e0b    cs2                       Eth1/1            N9K-
C92300YC
4 entries were displayed.



cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         144    H           FAS2980       e0a
node2              Eth1/2         145    H           FAS2980       e0a
cs2(FDO220329V5)   Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
cs2(FDO220329V5)   Eth1/66        176    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         139    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

Step 1: Prepare for replacement

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

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

   a. Go to the *NetApp Cluster and Management Network Switches Reference Configuration File Description Page* on the NetApp Support Site.
   b. Click the link for the *Cluster Network and Management Network Compatibility Matrix*, and then note the required switch software version.
   c. Click your browser's back arrow to return to the **Description** page, click **CONTINUE**, accept the license agreement, and then go to the **Download** page.
   d. Follow the steps on the Download page to download the correct RCF and NX-OS files for the version of ONTAP software you are installing.
2. On the new switch, log in as admin and shut down all of the ports that will be connected to the node cluster interfaces (ports 1/1 to 1/64).

   If the switch that you are replacing is not functional and is powered down, go to Step 4. The LIFs on the cluster nodes should have already failed over to the other cluster port for each node.

Show example

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-64
newcs2(config-if-range)# shutdown
```

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

```
network interface show -vserver Cluster -fields auto-revert
```

Show example

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

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

4 entries were displayed.
```

4. Verify that all the cluster LIFs can communicate:

```
cluster ping-cluster
```

Show example

```
cluster1::*> cluster ping-cluster node1

Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Step 2: Configure cables and ports

1. Shut down the ISL ports 1/65 and 1/66 on the Nexus 92300YC switch cs1:

Show example

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/65-66
cs1(config-if-range)# shutdown
cs1(config-if-range)#
```

2. Remove all of the cables from the Nexus 92300YC cs2 switch, and then connect them to the same ports on the Nexus 92300YC newcs2 switch.

3. Bring up the ISLs ports 1/65 and 1/66 between the cs1 and newcs2 switches, and then verify the port channel operation status.

   Port-Channel should indicate Po1(SU) and Member Ports should indicate Eth1/65(P) and Eth1/66(P).

   Show example

   This example enables ISL ports 1/65 and 1/66 and displays the port channel summary on switch cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/65-66
cs1(config-if-range)# no shutdown

cs1(config-if-range)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)

cs1(config-if-range)#
```

4. Verify that port e0b is up on all nodes:

```
network port show ipspace Cluster
```

Show example

The output should be similar to the following:

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

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- -----------
-------- -------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ----- -----------
-------- -------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/auto   -
false

4 entries were displayed.
```

5. On the same node you used in the previous step, revert the cluster LIF associated with the port in the previous step by using the network interface revert command.

Show example

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

The following commands return LIF `node1_clus2` on `node1` to home port `e0a` and displays information about the LIFs on both nodes. Bringing up the first node is successful if the Is Home column is true for both cluster interfaces and they show the correct port assignments, in this example `e0a` and `e0b` on node1.

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask      Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false

4 entries were displayed.
```

6. Display information about the nodes in a cluster:

`cluster show`

Show example

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

```
cluster1::*> cluster show

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

7. Verify that all physical cluster ports are up:

   `network port show ipspace Cluster`

   Show example

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

Node: node1

Ignore
                                                    Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- -----------
-------- ------
e0a       Cluster     Cluster           up    9000  auto/10000
healthy  false
e0b       Cluster     Cluster           up    9000  auto/10000
healthy  false

Node: node2

Ignore
                                                    Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link  MTU   Admin/Oper
Status   Status
--------- ------------ ---------------- ----- ----- -----------
-------- ------
e0a       Cluster      Cluster          up    9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up    9000  auto/10000
healthy  false

4 entries were displayed.
```

Step 3: Complete the procedure

1. Verify that all the cluster LIFs can communicate:

   `cluster ping-cluster`

Show example

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

2. Confirm the following cluster network configuration:

```
network port show
```

Show example

```
cluster1::*> network port show -ipspace Cluster
Node: node1

Ignore
                                       Speed(Mbps)            Health
Health
Port      IPspace     Broadcast Domain Link MTU   Admin/Oper  Status
Status
--------- ----------- ---------------- ---- ----- -----------
-------- ------
e0a       Cluster     Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster     Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                        Speed(Mbps)           Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000 auto/10000
healthy  false

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
```

```
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2              N9K-
C92300YC
            e0b    newcs2                    0/2              N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1              N9K-
C92300YC
            e0b    newcs2                    0/1              N9K-
C92300YC

4 entries were displayed.


cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID            Local Intrfce  Hldtme Capability  Platform
Port ID
node1                Eth1/1         144    H           FAS2980
e0a
node2                Eth1/2         145    H           FAS2980
e0a
newcs2(FDO296348FU)  Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
newcs2(FDO296348FU)  Eth1/66        176    R S I s     N9K-C92300YC
```

```
Eth1/66


Total entries displayed: 4


cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         139    H           FAS2980
e0b
node2              Eth1/2         124    H           FAS2980
e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

3. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files, using gthe commamds:

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

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.

Replace Cisco Nexus 92300YC 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.

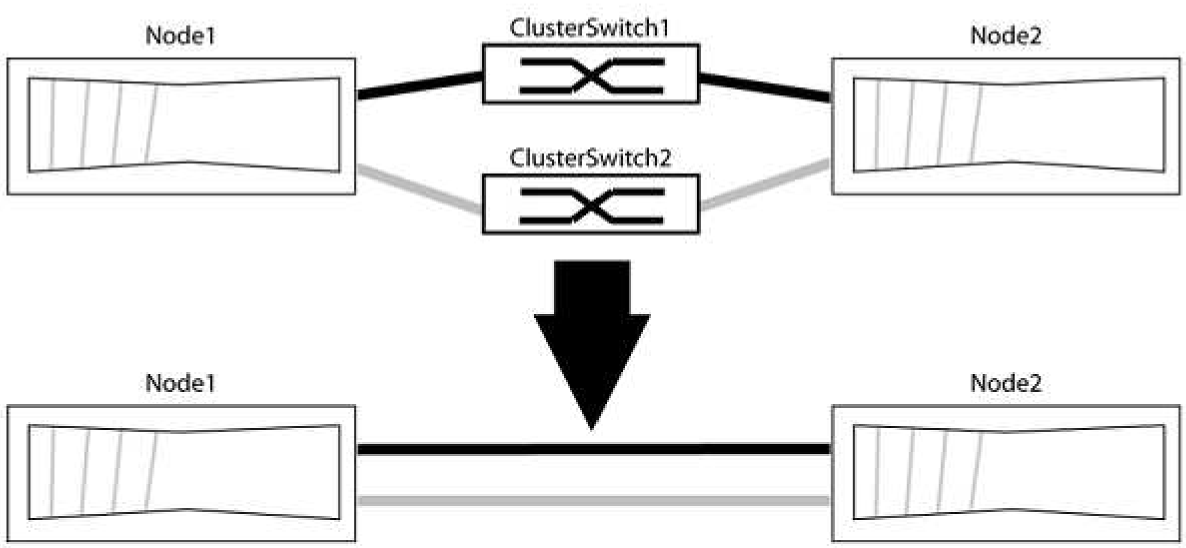
What you’ll need

- 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

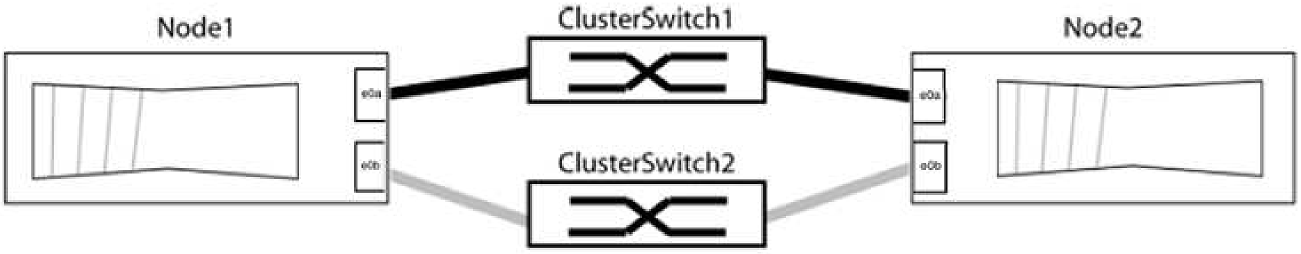
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

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`

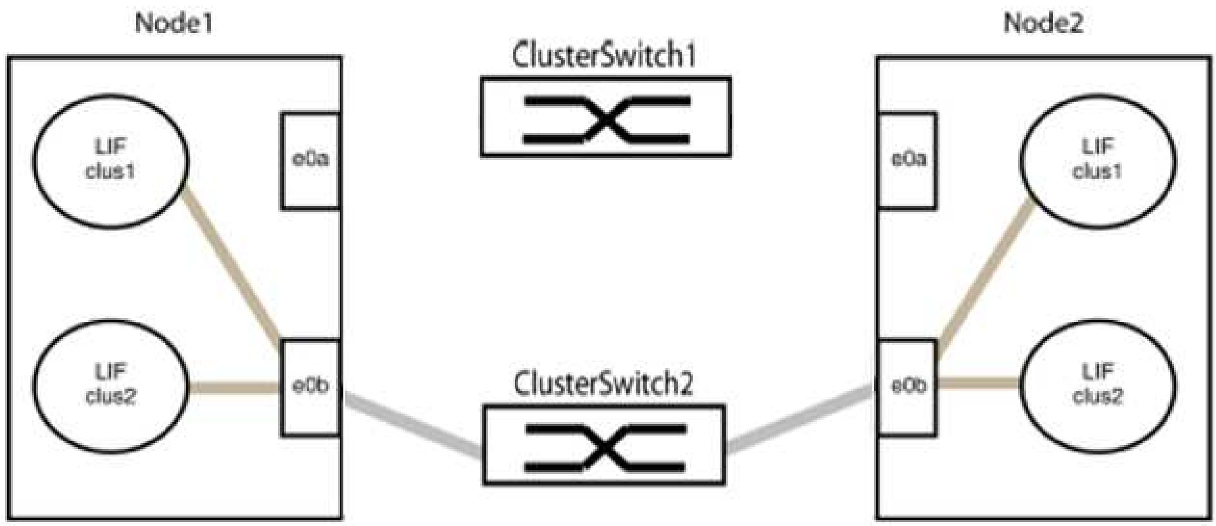
   All units must be either master or secondary.

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**.

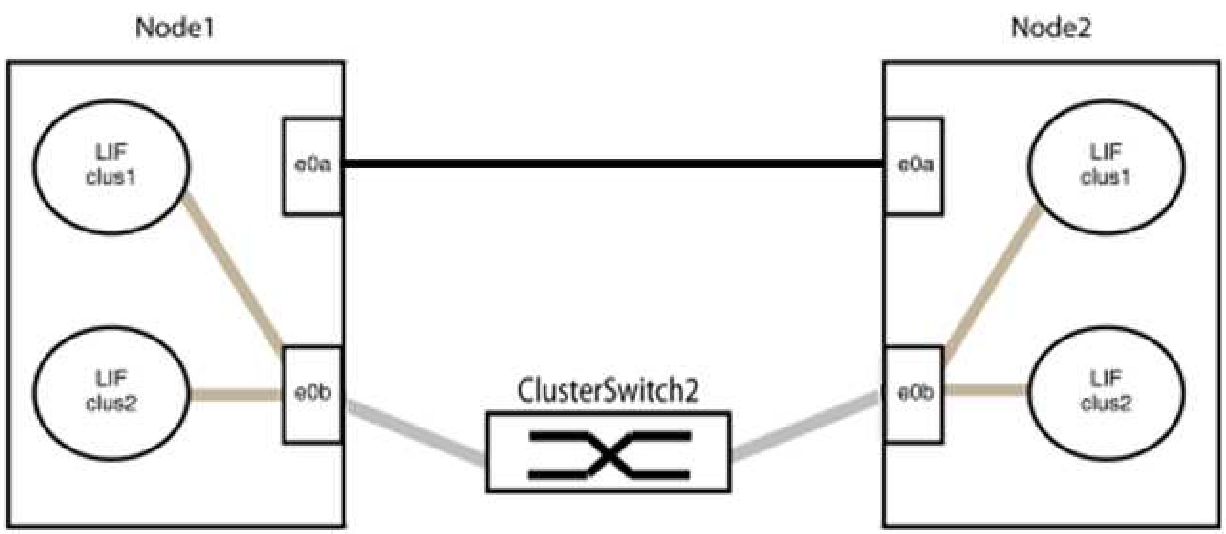
   a. Disconnect all the cables from the ports in group1 at the same time.

      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:



9. The switchless cluster network option transitions from `false` to `true`. This might take up to 45 seconds. Confirm that the switchless option is set to `true`:

   `network options switchless-cluster show`

   The following example shows that the switchless cluster is enabled:

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

10. Verify that the cluster network is not disrupted:

   `cluster ping-cluster -node local`

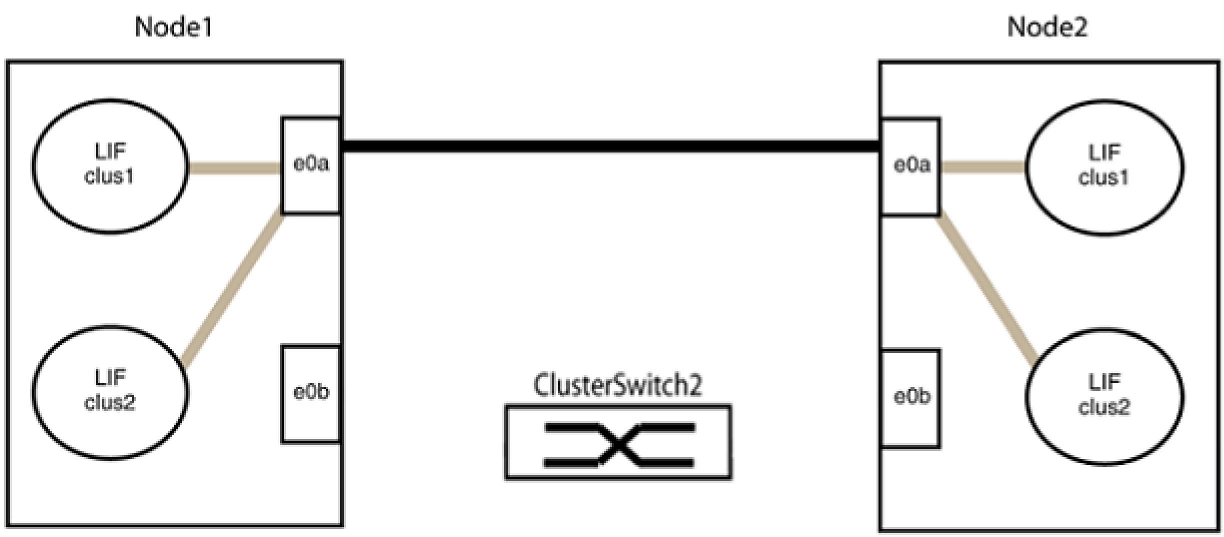
> **Note:** Before proceeding to the next step, you must wait at least two minutes to confirm a working back-to-back connection on group 1.

11. Set up the switchless configuration for the ports in group 2.

> **Note:** To avoid potential networking issues, you must disconnect the ports from group2 and reconnect them back-to-back as quickly as possible, for example, **in less than 20 seconds**.

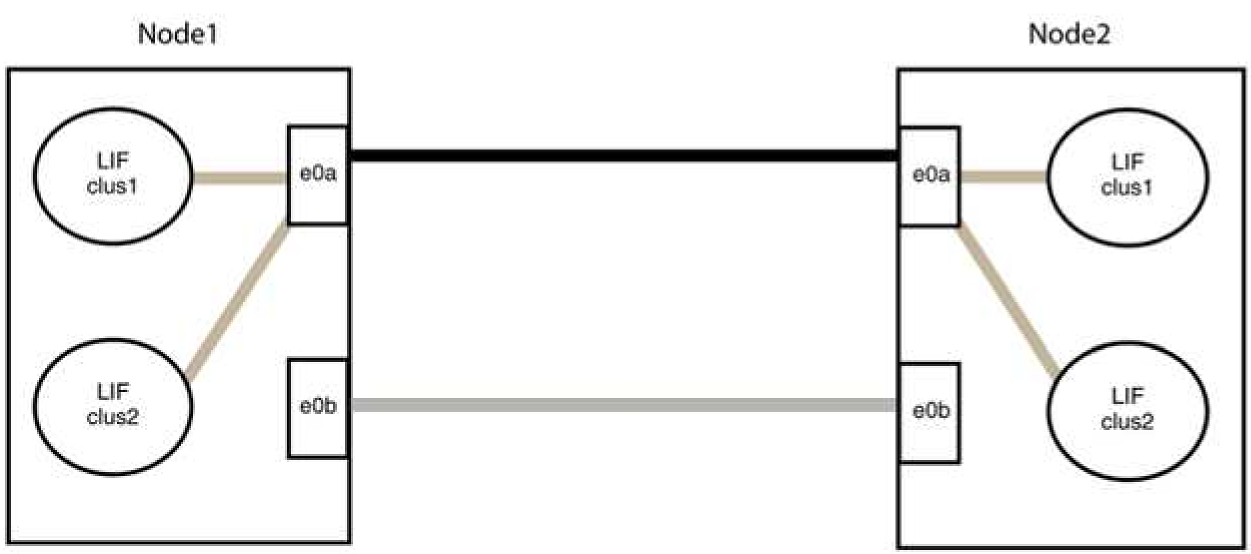
a. Disconnect all the cables from the ports in group2 at the same time.

In the following example, the cables are disconnected from port "e0b" on each node, and cluster traffic continues through the direct connection between the "e0a" ports:



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

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



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
```

NetApp CN1610

Overview of installation and configuration for NetApp CN1610 switches

The CN1610 is a high bandwidth, managed Layer 2 switch that provides 16 10-Gigabit Small Form-Factor Pluggable Plus (SFP+) ports.

The switch includes redundant power supplies and fan trays that support hot swapping for high availability. This 1U switch can be installed in a standard 19-inch NetApp 42U system cabinet or third-party cabinet.

The switch supports local management through the console port or remote management by using Telnet or SSH through a network connection. The CN1610 includes a dedicated 1-Gigabit Ethernet RJ45 management port for out-of-band switch management. You can manage the switch by entering commands into the command-line interface (CLI) or by using an SNMP-based network management system (NMS).

Install and configure workflow for NetApp CN1610 switches

To install and configure a NetApp CN1610 switch on systems running ONTAP, follow these steps:

1. Install hardware
2. Install FASTPATH software
3. Install Reference Configuration file

   If the switches are running ONTAP 8.3.1 or later, follow the instructions in Install FASTPATH and RCFs on switches running ONTAP 8.3.1 and later.

4. Configure switch

Documentation requirements for NetApp CN1610 switches

For NetApp CN1610 switch installation and maintenance, be sure to review all the recommended documentation.

Document title	Description
1G Installation Guide	An overview of the CN1601 switch hardware and software features and installation process.
10G Installation Guide	An overview of the CN1610 switch hardware and software features and describes the features to install the switch and access the CLI.
CN1601 and CN1610 Switch Setup and Configuration Guide	Details how to configure the switch hardware and software for your cluster environment.

Document title	Description
CN1601 Switch Administrator's Guide	Provides examples of how to use the CN1601 switch in a typical network. • Administrator's Guide • Administrator's Guide, Version 1.1.x.x • Administrator's Guide, Version 1.2.x.x
CN1610 Network Switch CLI Command Reference	Provides detailed information about the command-line interface (CLI) commands you use to configure the CN1601 software. • Command Reference • Command Reference, Version 1.1.x.x • Command Reference, Version 1.2.x.x

Install and configure

Install the hardware for the NetApp CN1610 switch

To install the NetApp CN1610 switch hardware, use the instructions in one of the following guides.

- 1G Installation Guide.

  An overview of the CN1601 switch hardware and software features and installation process.

- 10G Installation Guide

  An overview of the CN1610 switch hardware and software features and describes the features to install the switch and access the CLI.

Install FASTPATH software

When you install the FASTPATH software on your NetApp switches, you must begin the upgrade with the second switch, *cs2*.

Review requirements

What you'll need

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs and no defective cluster network interface cards (NICs) or similar issues).
- Fully functional port connections on the cluster switch.
- All cluster ports set up.
- All cluster logical interfaces (LIFs) set up (must not have been migrated).
- A successful communication path: The ONTAP (privilege: advanced) `cluster ping-cluster -node`

`node1` command must indicate that `larger than PMTU communication` is successful on all paths.

- A supported version of FASTPATH and ONTAP.

  Make sure you consult the switch compatibility table on the NetApp CN1601 and CN1610 Switches page for the supported FASTPATH and ONTAP versions.

Install FASTPATH

The following procedure uses the clustered Data ONTAP 8.2 syntax. As a result, the cluster Vserver, LIF names, and CLI output are different than those in Data ONTAP 8.3.

There can be command dependencies between command syntax in the RCF and FASTPATH versions.

About the examples

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

- The two NetApp switches are cs1 and cs2.
- The two cluster LIFs are clus1 and clus2.
- The Vservers are vs1 and vs2.
- The `cluster::*>` prompt indicates the name of the cluster.
- The cluster ports on each node are named e1a and e2a.

  Hardware Universe has more information about the actual cluster ports that are supported on your platform.

- The supported Inter-Switch Links (ISLs) are ports 0/13 through 0/16.
- The supported node connections are ports 0/1 through 0/12.

Step 1: Migrate cluster

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

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

   x is the duration of the maintenance window in hours.

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

2. Log into the switch as admin. There is no password by default. At the `(cs2) #` prompt, enter the `enable` command. Again, there is no password by default. This gives you access to Privileged EXEC mode, which allows you to configure the network interface.

Show example

```
(cs2) # enable
Password (Enter)
(cs2) #
```

3. On the console of each node, migrate clus2 to port e1a:

   `network interface migrate`

   Show example

```
cluster::*> network interface migrate -vserver vs1 -lif clus2
-destnode node1 -dest-port e1a
cluster::*> network interface migrate -vserver vs2 -lif clus2
-destnode node2 -dest-port e1a
```

4. On the console of each node, verify that the migration took place:

   `network interface show`

   The following example shows that clus2 has migrated to port e1a on both nodes:

   Show example

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

         Logical    Status     Network        Current  Current  Is
Vserver  Interface  Admin/Open Address/Mask   Node     Port     Home
-------- ---------- ---------- -------------- -------- -------  ----
vs1
         clus1      up/up      10.10.10.1/16  node1    e1a      true
         clus2      up/up      10.10.10.2/16  node1    e1a
false
vs2
         clus1      up/up      10.10.10.1/16  node2    e1a      true
         clus2      up/up      10.10.10.2/16  node2    e1a
false
```

Step 2: Install FASTPATH software

1. Shut down cluster port e2a on both nodes:

```
network port modify
```

Show example

The following example shows port e2a being shut down on both nodes:

```
cluster::*> network port modify -node node1 -port e2a -up-admin
false
cluster::*> network port modify -node node2 -port e2a -up-admin
false
```

2. Verify that port e2a is shut down on both nodes:

```
network port show
```

Show example

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

                                 Auto-Negot  Duplex      Speed
(Mbps)
Node   Port Role     Link MTU    Admin/Oper  Admin/Oper  Admin/Oper
------ ---- -------- ---- -----  ----------  ----------
------------
node1
       e1a  cluster  up   9000   true/true   full/full   auto/10000
       e2a  cluster  down 9000   true/true   full/full   auto/10000
node2
       e1a  cluster  up   9000   true/true   full/full   auto/10000
       e2a  cluster  down 9000   true/true   full/full   auto/10000
```

3. Shut down the Inter-Switch Link (ISL) ports on cs1, the active NetApp switch:

Show example

```
(cs1) # configure
(cs1)(config) # interface 0/13-0/16
(cs1)(Interface 0/13-0/16) # shutdown
(cs1)(Interface 0/13-0/16) # exit
(cs1)(config) # exit
```

4. Back up the current active image on cs2.

Show example

```
(cs2) # show bootvar

 Image Descriptions   .

  active:
  backup:

 Images currently available on Flash

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

    1        1.1.0.3      1.1.0.1         1.1.0.3           1.1.0.3

(cs2) # copy active backup
Copying active to backup
Copy operation successful

(cs2) #
```

5. Download the image file to the switch.

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

Show example

```
(cs2) # copy tftp://10.0.0.1/NetApp_CN1610_1.1.0.5.stk active


Mode...................................... TFTP
Set Server IP............................. 10.0.0.1
Path...................................... ./
Filename.................................. NetApp_CN1610_1.1.0.5.stk
Data Type................................. Code
Destination Filename...................... active

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


File transfer operation completed successfully.
```

6. Verify the running version of the FASTPATH software.

```
show version
```

Show example

```
(cs2) # show version

Switch: 1

System Description................. Broadcom Scorpion 56820
                                    Development System - 16 TENGIG,
                                    1.1.0.3, Linux 2.6.21.7
Machine Type....................... Broadcom Scorpion 56820
                                    Development System - 16TENGIG
Machine Model...................... BCM-56820
Serial Number...................... 10611100004
FRU Number.........................
Part Number........................ BCM56820
Maintenance Level.................. A
Manufacturer....................... 0xbc00
Burned In MAC Address.............. 00:A0:98:4B:A9:AA
Software Version................... 1.1.0.3
Operating System................... Linux 2.6.21.7
Network Processing Device.......... BCM56820_B0
Additional Packages................ FASTPATH QOS
                                    FASTPATH IPv6 Management
```

7. View the boot images for the active and backup configuration.

   `show bootvar`

Show example

```
(cs2) # show bootvar

Image Descriptions

 active :
 backup :

 Images currently available on Flash

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

    1        1.1.0.3      1.1.0.3         1.1.0.3           1.1.0.5
```

8. Reboot the switch.

   `reload`

   Show example

```
(cs2) # reload

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

System will now restart!
```

Step 3: Validate installation

1. Log in again, and verify the new version of the FASTPATH software.

   `show version`

Show example

```
(cs2) # show version

Switch: 1

System Description................... Broadcom Scorpion 56820
                                      Development System - 16
TENGIG,
                                      1.1.0.5, Linux 2.6.21.7
Machine Type......................... Broadcom Scorpion 56820
                                      Development System - 16TENGIG
Machine Model........................ BCM-56820
Serial Number........................ 10611100004
FRU Number...........................
Part Number.......................... BCM56820
Maintenance Level.................... A
Manufacturer......................... 0xbc00
Burned In MAC Address................ 00:A0:98:4B:A9:AA
Software Version..................... 1.1.0.5
Operating System..................... Linux 2.6.21.7
Network Processing Device............ BCM56820_B0
Additional Packages.................. FASTPATH QOS
                                      FASTPATH IPv6 Management
```

2. Bring up the ISL ports on cs1, the active switch.

   `configure`

   Show example

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (Interface 0/13-0/16) # no shutdown
(cs1) (Interface 0/13-0/16) # exit
(cs1) (config) # exit
```

3. Verify that the ISLs are operational:

   `show port-channel 3/1`

   The Link State field should indicate `Up`.

Show example

```
(cs2) # show port-channel 3/1

Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  True
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

4. Copy the `running-config` file to the `startup-config` file when you are satisfied with the software versions and switch settings.

Show example

```
(cs2) # write memory

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

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

Config file 'startup-config' created successfully .

Configuration Saved!
```

5. Enable the second cluster port, e2a, on each node:

`network port modify`

Show example

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> **network port modify -node node2 -port e2a -up-admin
true**
```

6. Revert clus2 that is associated with port e2a:

   `network interface revert`

   The LIF might revert automatically, depending on your version of ONTAP software.

   Show example

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

7. Verify that the LIF is now home (`true`) on both nodes:

   `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
-------- ---------- ---------- -------------- -------- ------- ----
vs1
         clus1      up/up      10.10.10.1/24  node1    e1a     true
         clus2      up/up      10.10.10.2/24  node1    e2a     true
vs2
         clus1      up/up      10.10.10.1/24  node2    e1a     true
         clus2      up/up      10.10.10.2/24  node2    e2a     true
```

8. View the status of the nodes:

   `cluster show`

Show example

```
cluster::> cluster show

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

9. Repeat the previous steps to install the FASTPATH software on the other switch, cs1.
10. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

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

Install a Reference Configuration File on a CN1610 switch

Follow this procedure to install a Reference Configuration File (RCF).

Before installing an RCF, you must first migrate the cluster LIFs away from switch cs2. After the RCF is installed and validated, the LIFs can be migrated back.

Review requirements

What you'll need

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs and no defective cluster network interface cards (NICs) or similar issues).
- Fully functional port connections on the cluster switch.
- All cluster ports set up.
- All cluster logical interfaces (LIFs) set up.
- A successful communication path: The ONTAP (privilege: advanced) `cluster ping-cluster -node node1` command must indicate that `larger than PMTU communication` is successful on all paths.
- A supported version of RCF and ONTAP.

  Make sure you consult the switch compatibility table on the NetApp CN1601 and CN1610 Switches page for the supported RCF and ONTAP versions.

Install the RCF

The following procedure uses the clustered Data ONTAP 8.2 syntax. As a result, the cluster Vserver, LIF names, and CLI output are different than those in Data ONTAP 8.3.

There can be command dependencies between command syntax in the RCF and FASTPATH versions.

In RCF version 1.2, support for Telnet has been explicitly disabled because of security concerns. To avoid connectivity issues while installing RCF 1.2, verify that Secure Shell (SSH) is enabled. The NetApp CN1610 Switch Administrator's Guide has more information about SSH.

About the examples

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

- The two NetApp switches are cs1 and cs2.
- The two cluster LIFs are clus1 and clus2.
- The Vservers are vs1 and vs2.
- The `cluster::*>` prompt indicates the name of the cluster.
- The cluster ports on each node are named e1a and e2a.

  Hardware Universe has more information about the actual cluster ports that are supported on your platform.
- The supported Inter-Switch Links (ISLs) are ports 0/13 through 0/16.
- The supported node connections are ports 0/1 through 0/12.
- A supported version of FASTPATH, RCF, and ONTAP.

  Make sure you consult the switch compatibility table on the NetApp CN1601 and CN1610 Switches page for the supported FASTPATH, RCF, and ONTAP versions.

Step 1: Migrate cluster

1. Save your current switch configuration information:

   `write memory`

   Show example

   The following example shows the current switch configuration being saved to the startup configuration (`startup-config`) file on switch cs2:

   ```
   (cs2) # write memory
   This operation may take a few minutes.
   Management interfaces will not be available during this time.

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

   Config file 'startup-config' created successfully.

   Configuration Saved!
   ```

2. On the console of each node, migrate clus2 to port e1a:

`network interface migrate`

Show example

```
cluster::*> network interface migrate -vserver vs1 -lif clus2
-source-node node1 -destnode node1 -dest-port e1a

cluster::*> network interface migrate -vserver vs2 -lif clus2
-source-node node2 -destnode node2 -dest-port e1a
```

3. On the console of each node, verify that the migration occurred:

   `network interface show -role cluster`

   Show example

   The following example shows that clus2 has migrated to port e1a on both nodes:

```
cluster::*> network port show -role cluster
         clus1      up/up      10.10.10.1/16   node2    e1a     true
         clus2      up/up      10.10.10.2/16   node2    e1a
false
```

4. Shut down port e2a on both nodes:

   `network port modify`

   Show example

   The following example shows port e2a being shut down on both nodes:

```
cluster::*> network port modify -node node1 -port e2a -up-admin
false
cluster::*> network port modify -node node2 -port e2a -up-admin
false
```

5. Verify that port e2a is shut down on both nodes:

   `network port show`

Show example

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

                                        Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role     Link MTU   Admin/Oper  Admin/Oper  Admin/Oper
------ ------ -------- ---- ----- ----------- ----------
-----------
node1
       e1a    cluster  up   9000  true/true   full/full   auto/10000
       e2a    cluster  down 9000  true/true   full/full   auto/10000
node2
       e1a    cluster  up   9000  true/true   full/full   auto/10000
       e2a    cluster  down 9000  true/true   full/full   auto/10000
```

6. Shut down the ISL ports on cs1, the active NetApp switch.

Show example

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (interface 0/13-0/16) # shutdown
(cs1) (interface 0/13-0/16) # exit
(cs1) (config) # exit
```

Step 2: Install RCF

1. Copy the RCF to the switch.

   You must set the `.scr` extension as part of the file name before invoking the script. This extension is the extension for the FASTPATH operating system.

   The switch will validate the script automatically as it is downloaded to the switch, and the output will go to the console.

Show example

```
(cs2) # copy tftp://10.10.0.1/CN1610_CS_RCF_v1.1.txt nvram:script
CN1610_CS_RCF_v1.1.scr

[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```

2. Verify that the script was downloaded and saved with the file name that you gave it.

Show example

```
(cs2) # script list
Configuration Script Name        Size(Bytes)
-------------------------------- -----------
running-config.scr               6960
CN1610_CS_RCF_v1.1.scr           2199

2 configuration script(s) found.
6038 Kbytes free.
```

3. Validate the script.

> ℹ The script is validated during the download to verify that each line is a valid switch command line.

Show example

```
(cs2) # script validate CN1610_CS_RCF_v1.1.scr
[the script is now displayed line by line]
Configuration script 'CN1610_CS_RCF_v1.1.scr' validated.
```

4. Apply the script to the switch.

Show example

```
(cs2) #script apply CN1610_CS_RCF_v1.1.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.1.scr' applied.
```

5. Verify that your changes have been implemented on the switch.

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

The example displays the `running-config` file on the switch. You must compare the file to the RCF to verify that the parameters that you set are as you expect.

6. Save the changes.
7. Set the `running-config` file to be the standard one.

Show example

```
(cs2) # write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.
```

8. Reboot the switch and verify that the `running-config` file is correct.

After the reboot completes, you must log in, view the `running-config` file, and then look for the description on interface 3/64, which is the version label for the RCF.

Show example

```
(cs2) # reload

The system has unsaved changes.
Would you like to save them now? (y/n) y


Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

9. Bring up the ISL ports on cs1, the active switch.

   Show example

```
(cs1) # configure
(cs1) (config)# interface 0/13-0/16
(cs1) (Interface 0/13-0/16)# no shutdown
(cs1) (Interface 0/13-0/16)# exit
(cs1) (config)# exit
```

10. Verify that the ISLs are operational:

    `show port-channel 3/1`

    The Link State field should indicate `Up`.

Show example

```
(cs2) # show port-channel 3/1

Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  True
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

11. Bring up cluster port e2a on both nodes:

    `network port modify`

    Show example

    The following example shows port e2a being brought up on node1 and node2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

Step 3: Validate installation

1. Verify that port e2a is up on both nodes:

   `network port show -role cluster`

Show example

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

                                  Auto-Negot  Duplex      Speed (Mbps)
Node   Port Role     Link MTU   Admin/Oper  Admin/Oper  Admin/Oper
------ ---- -------- ---- ----  ----------- ----------  ------------
node1
       e1a  cluster  up   9000  true/true   full/full   auto/10000
       e2a  cluster  up   9000  true/true   full/full   auto/10000
node2
       e1a  cluster  up   9000  true/true   full/full   auto/10000
       e2a  cluster  up   9000  true/true   full/full   auto/10000
```

2. On both nodes, revert clus2 that is associated with port e2a:

   `network interface revert`

   The LIF might revert automatically, depending on your version of ONTAP.

Show example

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```

3. Verify that the LIF is now home (`true`) on both nodes:

   `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
------- ---------- ---------- -------------- -------- ------- ----
vs1
        clus1      up/up      10.10.10.1/24  node1    e1a     true
        clus2      up/up      10.10.10.2/24  node1    e2a     true
vs2
        clus1      up/up      10.10.10.1/24  node2    e1a     true
        clus2      up/up      10.10.10.2/24  node2    e2a     true
```

4. View the status of the node members:

   `cluster show`

   Show example

   ```
   cluster::> cluster show

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

5. Copy the `running-config` file to the `startup-config` file when you are satisfied with the software versions and switch settings.

   Show example

   ```
   (cs2) # write memory
   This operation may take a few minutes.
   Management interfaces will not be available during this time.

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

   Config file 'startup-config' created successfully.

   Configuration Saved!
   ```

6. Repeat the previous steps to install the RCF on the other switch, cs1.

Install FASTPATH software and RCFs for ONTAP 8.3.1 and later

Follow this procedure to install FASTPATH software and RCFs for ONTAP 8.3.1 and later.

The installation steps are the same for both NetApp CN1601 management switches and CN1610 cluster switches running ONTAP 8.3.1 or later. However, the two models require different software and RCFs.

Review requirements

What you'll need

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs and no defective cluster network interface cards (NICs) or similar issues).

- Fully functional port connections on the cluster switch.
- All cluster ports set up.
- All cluster logical interfaces (LIFs) set up (must not have been migrated).
- A successful communication path: The ONTAP (privilege: advanced) `cluster ping-cluster -node node1` command must indicate that `larger than PMTU communication` is successful on all paths.
- A supported version of FASTPATH, RCF, and ONTAP.

  Make sure you consult the switch compatibility table on the NetApp CN1601 and CN1610 Switches page for the supported FASTPATH, RCF, and ONTAP versions.

Install the FASTPATH software

The following procedure uses the clustered Data ONTAP 8.2 syntax. As a result, the cluster Vserver, LIF names, and CLI output are different than those in Data ONTAP 8.3.

There can be command dependencies between command syntax in the RCF and FASTPATH versions.

> In RCF version 1.2, support for Telnet has been explicitly disabled because of security concerns. To avoid connectivity issues while installing RCF 1.2, verify that Secure Shell (SSH) is enabled. The NetApp CN1610 Switch Administrator's Guide has more information about SSH.

About the examples

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

- The two NetApp switch names are cs1 and cs2.
- The cluster logical interface (LIF) names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2. (You can have up to 24 nodes in a cluster.)
- The storage virtual machine (SVM) name is Cluster.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The cluster ports on each node are named e0a and e0b.

  Hardware Universe has more information about the actual cluster ports that are supported on your platform.

- The supported Inter-Switch Links (ISLs) are ports 0/13 through 0/16.
- The supported node connections are ports 0/1 through 0/12.

Step 1: Migrate cluster

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

   ```
   network port show -ipspace cluster
   ```

Show example

The following example shows the type of output from the command:

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

2. Display information about the LIFs on the cluster:

`network interface show -role cluster`

Show example

The following example shows the logical interfaces on the cluster. In this example the `-role` parameter displays information about the LIFs that are associated with cluster ports:

```
cluster1::> network interface show -role cluster
  (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    10.254.66.82/16    node1
e0a     true
            node1_clus2  up/up    10.254.206.128/16  node1
e0b     true
            node2_clus1  up/up    10.254.48.152/16   node2
e0a     true
            node2_clus2  up/up    10.254.42.74/16    node2
e0b     true
4 entries were displayed.
```

3. On each respective node, using a node management LIF, migrate node1_clus2 to e0a on node1 and node2_clus2 to e0a on node2:

   `network interface migrate`

   You must enter the commands on the controller consoles that own the respective cluster LIFs.

   Show example

```
cluster1::> network interface migrate -vserver Cluster -lif
node1_clus2 -destination-node node1 -destination-port e0a
cluster1::> network interface migrate -vserver Cluster -lif
node2_clus2 -destination-node node2 -destination-port e0a
```

   For this command, the name of the cluster is case-sensitive and the command should be run on each node. It is not possible to run this command in the general cluster LIF.

4. Verify that the migration took place by using the `network interface show` command on a node.

Show example

The following example shows that clus2 has migrated to port e0a on nodes node1 and node2:

```
cluster1::> **network interface show -role cluster**
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    10.254.66.82/16   node1
e0a     true
            node1_clus2  up/up    10.254.206.128/16 node1
e0a     false
            node2_clus1  up/up    10.254.48.152/16  node2
e0a     true
            node2_clus2  up/up    10.254.42.74/16   node2
e0a     false
4 entries were displayed.
```

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

   `set -privilege advanced`

   The advanced prompt (*>) appears.

6. Shut down cluster port e0b on both nodes:

   `network port modify -node` *`node_name`* `-port` *`port_name`* `-up-admin false`

   You must enter the commands on the controller consoles that own the respective cluster LIFs.

   Show example

   The following example shows the commands to shut down port e0b on all nodes:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin
false
cluster1::*> network port modify -node node2 -port e0b -up-admin
false
```

7. Verify that port e0b is shut down on both nodes:

```
network port show
```

Show example

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

                                                                 Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          down     9000
auto/10000
node2
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          down     9000
auto/10000
4 entries were displayed.
```

8. Shut down the Inter-Switch Link (ISL) ports on cs1.

Show example

```
(cs1) #configure
(cs1) (Config)#interface 0/13-0/16
(cs1) (Interface 0/13-0/16)#shutdown
(cs1) (Interface 0/13-0/16)#exit
(cs1) (Config)#exit
```

9. Back up the current active image on cs2.

Show example

```
(cs2) # show bootvar

 Image Descriptions

 active :
 backup :


 Images currently available on Flash

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

    1     1.1.0.5     1.1.0.3           1.1.0.5             1.1.0.5

(cs2) # copy active backup
Copying active to backup
Copy operation successful
```

Step 2: Install the FASTPATH software and RCF

1. Verify the running version of the FASTPATH software.

Show example

```
(cs2) # show version

Switch: 1

System Description............................. NetApp CN1610,
1.1.0.5, Linux
                                                2.6.21.7
Machine Type................................... NetApp CN1610
Machine Model.................................. CN1610
Serial Number.................................. 20211200106
Burned In MAC Address.......................... 00:A0:98:21:83:69
Software Version............................... 1.1.0.5
Operating System............................... Linux 2.6.21.7
Network Processing Device...................... BCM56820_B0
Part Number.................................... 111-00893

--More-- or (q)uit


Additional Packages............................ FASTPATH QOS
                                                FASTPATH IPv6
Management
```

2. Download the image file to the switch.

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

Show example

```
(cs2) #copy
sftp://root@10.22.201.50//tftpboot/NetApp_CN1610_1.2.0.7.stk active
Remote Password:********

Mode........................................... SFTP
Set Server IP.................................. 10.22.201.50
Path........................................... /tftpboot/
Filename.......................................
NetApp_CN1610_1.2.0.7.stk
Data Type...................................... Code
Destination Filename........................... active

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


File transfer operation completed successfully.
```

3. Confirm the current and next-active boot image versions:

`show bootvar`

Show example

```
(cs2) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

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


    1     1.1.0.8     1.1.0.8           1.1.0.8           1.2.0.7
```

4. Install the compatible RCF for the new image version to the switch.

   If the RCF version is already correct, bring up the ISL ports.

   Show example

```
(cs2) #copy tftp://10.22.201.50//CN1610_CS_RCF_v1.2.txt nvram:script
CN1610_CS_RCF_v1.2.scr

Mode........................................... TFTP
Set Server IP.................................. 10.22.201.50
Path........................................... /
Filename.......................................
CN1610_CS_RCF_v1.2.txt
Data Type...................................... Config Script
Destination Filename...........................
CN1610_CS_RCF_v1.2.scr

File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.


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


Validating configuration script...
[the script is now displayed line by line]

Configuration script validated.
File transfer operation completed successfully.
```

   The `.scr` extension must be set as part of the file name before invoking the script. This extension is for the FASTPATH operating system.

   The switch validates the script automatically as it is downloaded to the switch. The output goes to the console.

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

Show example

```
(cs2) #script list

Configuration Script Name        Size(Bytes)
-------------------------------- -----------
CN1610_CS_RCF_v1.2.scr                  2191

1 configuration script(s) found.
2541 Kbytes free.
```

6. Apply the script to the switch.

Show example

```
(cs2) #script apply CN1610_CS_RCF_v1.2.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.2.scr' applied.
```

7. Verify that the changes have been applied to the switch, and then save them:

`show running-config`

Show example

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

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

Show example

```
(cs2) #write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.

Configuration Saved!
```

9. Reboot the switch.

Show example

```
(cs2) #reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

Step 3: Validate installation

1. Log in again, and then verify that the switch is running the new version of the FASTPATH software.

Show example

```
(cs2) #show version

Switch: 1

System Description............................. NetApp CN1610,
1.2.0.7,Linux
                                                3.8.13-4ce360e8
Machine Type................................... NetApp CN1610
Machine Model.................................. CN1610
Serial Number.................................. 20211200106
Burned In MAC Address.......................... 00:A0:98:21:83:69
Software Version............................... 1.2.0.7
Operating System............................... Linux 3.8.13-
4ce360e8
Network Processing Device...................... BCM56820_B0
Part Number.................................... 111-00893
CPLD version................................... 0x5


Additional Packages............................ FASTPATH QOS
                                                FASTPATH IPv6
Management
```

After the reboot completes, you must log in to verify the image version, view the running configuration, and look for the description on interface 3/64, which is the version label for the RCF.

2. Bring up the ISL ports on cs1, the active switch.

Show example

```
(cs1) #configure
(cs1) (Config) #interface 0/13-0/16
(cs1) (Interface 0/13-0/16) #no shutdown
(cs1) (Interface 0/13-0/16) #exit
(cs1) (Config) #exit
```

3. Verify that the ISLs are operational:

`show port-channel 3/1`

The Link State field should indicate `Up`.

Show example

```
(cs1) #show port-channel 3/1

Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  False
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

4. Bring up cluster port e0b on all nodes:

`network port modify`

You must enter the commands on the controller consoles that own the respective cluster LIFs.

Show example

The following example shows port e0b being brought up on node1 and node2:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin
true
cluster1::*> network port modify -node node2 -port e0b -up-admin
true
```

5. Verify that the port e0b is up on all nodes:

`network port show -ipspace cluster`

Show example

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

                                                             Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU
Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          up       9000
auto/10000
node2
       e0a       Cluster      Cluster          up       9000
auto/10000
       e0b       Cluster      Cluster          up       9000
auto/10000
4 entries were displayed.
```

6. Verify that the LIF is now home (`true`) on both nodes:

   `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
            node1_clus1  up/up    169.254.66.82/16   node1
e0a     true
            node1_clus2  up/up    169.254.206.128/16 node1
e0b     true
            node2_clus1  up/up    169.254.48.152/16  node2
e0a     true
            node2_clus2  up/up    169.254.42.74/16   node2
e0b     true
4 entries were displayed.
```

7. Show the status of the node members:

`cluster show`

Show example

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          false
node2                true    true          false
2 entries were displayed.
```

8. Return to the admin privilege level:

`set -privilege admin`

9. Repeat the previous steps to install the FASTPATH software and RCF on the other switch, cs1.

Configure the hardware for the NetApp CN1610 switch

To configure the switch hardware and software for your cluster environment, refer to the

CN1601 and CN1610 Switch Setup and Configuration Guide.

Migrate switches

Migrate from a switchless cluster environment to a switched NetApp CN1610 cluster environment

If you have an existing two-node switchless cluster environment, you can migrate to a two-node switched cluster environment using CN1610 cluster network switches that enables you to scale beyond two nodes.

Review requirements

What you'll need

For a two-node switchless configuration, ensure that:

- The two-node switchless configuration is properly set up and functioning.
- The nodes are running ONTAP 8.2 or later.
- All cluster ports are in the `up` state.
- All cluster logical interfaces (LIFs) are in the `up` state and on their home ports.

For the CN1610 cluster switch configuration:

- The CN1610 cluster switch infrastructure are fully functional on both switches.
- Both switches have management network connectivity.
- There is console access to the cluster switches.
- CN1610 node-to-node switch and switch-to-switch connections use twinax or fiber cables.

  The Hardware Universe contains more information about cabling.

- Inter-Switch Link (ISL) cables are connected to ports 13 through 16 on both CN1610 switches.
- Initial customization of both the CN1610 switches are completed.

  Any previous site customization, such as SMTP, SNMP, and SSH should be copied to the new switches.

Related information

- Hardware Universe
- NetApp CN1601 and CN1610 description page
- CN1601 and CN1610 Switch Setup and Configuration Guide
- NetApp KB Article 1010449: How to suppress automatic case creation during scheduled maintenance windows

Migrate the switches

About the examples

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

- The names of the CN1610 switches are cs1 and cs2.

- The names of the LIFs are clus1 and clus2.
- The names of the nodes are node1 and node2.
- The `cluster::*>` prompt indicates the name of the cluster.
- The cluster ports used in this procedure are e1a and e2a.

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

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. 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.

   Show example

   The following command suppresses automatic case creation for two hours:

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

Step 2: Configure ports

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

   You must not disable the ISL ports.

Show example

The following example shows that node-facing ports 1 through 12 are disabled on switch cs1:

```
(cs1)> enable
(cs1)# configure
(cs1)(Config)# interface 0/1-0/12
(cs1)(Interface 0/1-0/12)# shutdown
(cs1)(Interface 0/1-0/12)# exit
(cs1)(Config)# exit
```

The following example shows that node-facing ports 1 through 12 are disabled on switch cs2:

```
(c2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

2. Verify that the ISL and the physical ports on the ISL between the two CN1610 cluster switches cs1 and cs2 are `up`:

   `show port-channel`

Show example

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

```
(cs1)# show port-channel 3/1
Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  True
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

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

```
(cs2)# show port-channel 3/1
Local Interface................................ 3/1
Channel Name................................... ISL-LAG
Link State..................................... Up
Admin Mode..................................... Enabled
Type........................................... Static
Load Balance Option............................ 7
(Enhanced hashing mode)

Mbr    Device/       Port      Port
Ports  Timeout       Speed     Active
------ ------------- --------- -------
0/13   actor/long    10G Full  True
       partner/long
0/14   actor/long    10G Full  True
       partner/long
0/15   actor/long    10G Full  True
       partner/long
0/16   actor/long    10G Full  True
       partner/long
```

3. Display the list of neighboring devices:

   `show isdp neighbors`

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

Show example

The following example lists the neighboring devices on switch cs1:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID              Intf         Holdtime  Capability   Platform
Port ID
---------------------- ------------ --------- ------------ ---------
------------
cs2                    0/13         11        S            CN1610
0/13
cs2                    0/14         11        S            CN1610
0/14
cs2                    0/15         11        S            CN1610
0/15
cs2                    0/16         11        S            CN1610
0/16
```

The following example lists the neighboring devices on switch cs2:

```
(cs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID              Intf         Holdtime  Capability   Platform
Port ID
---------------------- ------------ --------- ------------ ---------
------------
cs1                    0/13         11        S            CN1610
0/13
cs1                    0/14         11        S            CN1610
0/14
cs1                    0/15         11        S            CN1610
0/15
cs1                    0/16         11        S            CN1610
0/16
```

4. Display the list of cluster ports:

`network port show`

Show example

The following example shows the available cluster ports:

```
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
e0c       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0d       Cluster      Cluster          up   9000  auto/10000
healthy  false
e4a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e4b       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
e0c       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0d       Cluster      Cluster          up   9000  auto/10000
healthy  false
e4a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e4b       Cluster      Cluster          up   9000  auto/10000
healthy  false
12 entries were displayed.
```

5. Verify that each cluster port is connected to the corresponding port on its partner cluster node:

   ```
   run * cdpd show-neighbors
   ```

   Show example

   The following example shows that cluster ports e1a and e2a are connected to the same port on their cluster partner node:

   ```
   cluster::*> run * cdpd show-neighbors
   2 entries were acted on.

   Node: node1
   Local  Remote          Remote                 Remote           Hold
   Remote
   Port   Device          Interface              Platform         Time
   Capability
   ------ --------------- ---------------------- ---------------- -----
   ----------
   e1a    node2           e1a                    FAS3270           137
   H
   e2a    node2           e2a                    FAS3270           137
   H


   Node: node2

   Local  Remote          Remote                 Remote           Hold
   Remote
   Port   Device          Interface              Platform         Time
   Capability
   ------ --------------- ---------------------- ---------------- -----
   ----------
   e1a    node1           e1a                    FAS3270           161
   H
   e2a    node1           e2a                    FAS3270           161
   H
   ```

6. Verify that all of the cluster LIFs are `up` and operational:

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

   Each cluster LIF should display `true` in the “Is Home” column.

Show example

```
cluster::*> network interface show -vserver Cluster
            Logical    Status     Network       Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask  Node          Port
Home
----------- ---------- ---------- ------------- -------------
------- ----
node1
            clus1      up/up      10.10.10.1/16 node1         e1a
true
            clus2      up/up      10.10.10.2/16 node1         e2a
true
node2
            clus1      up/up      10.10.11.1/16 node2         e1a
true
            clus2      up/up      10.10.11.2/16 node2         e2a
true

4 entries were displayed.
```

The following modification and migration commands in steps 10 through 13 must be done from the local node.

7. Verify that all cluster ports are `up`:

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

Show example

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

                                         Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link  MTU   Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ----- ----- ----------- ----------
------------
node1
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000
node2
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

8. Set the `-auto-revert` parameter to `false` on cluster LIFs clus1 and clus2 on both nodes:

   `network interface modify`

   Show example

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```

   For release 8.3 and later, use the following command: `network interface modify -vserver Cluster -lif * -auto-revert false`

9. Ping the cluster ports to verify the cluster connectivity:

`cluster ping-cluster local`

The command output shows connectivity between all of the cluster ports.

10. Migrate clus1 to port e2a on the console of each node:

    `network interface migrate`

    Show example

    The following example shows the process for migrating clus1 to port e2a on node1 and node2:

    ```
    cluster::*> network interface migrate -vserver node1 -lif clus1
    -source-node node1 -dest-node node1 -dest-port e2a
    cluster::*> network interface migrate -vserver node2 -lif clus1
    -source-node node2 -dest-node node2 -dest-port e2a
    ```

    > For release 8.3 and later, use the following command: `network interface migrate -vserver Cluster -lif clus1 -destination-node node1 -destination -port e2a`

11. Verify that the migration took place:

    `network interface show -vserver Cluster`

Show example

The following example verifies that clus1 is migrated to port e2a on node1 and node2:

```
cluster::*> network interface show -vserver Cluster
            Logical    Status     Network       Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask  Node          Port
Home
----------- ---------- ---------- ------------- -------------
------- ----
node1
            clus1      up/up    10.10.10.1/16   node1         e2a
false
            clus2      up/up    10.10.10.2/16   node1         e2a
true
node2
            clus1      up/up    10.10.11.1/16   node2         e2a
false
            clus2      up/up    10.10.11.2/16   node2         e2a
true

4 entries were displayed.
```

12. Shut down cluster port e1a on both nodes:

    `network port modify`

    Show example

    The following example shows how to shut down the port e1a on node1 and node2:

```
cluster::*> network port modify -node node1 -port e1a -up-admin
false
cluster::*> network port modify -node node2 -port e1a -up-admin
false
```

13. Verify the port status:

    `network port show`

Show example

The following example shows that port e1a is `down` on node1 and node2:

```
cluster::*> network port show -role cluster
                                             Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link   MTU Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ---- ----- ----------- ----------
------------
node1
       e1a    clus1        down  9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000
node2
       e1a    clus1        down  9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

14. Disconnect the cable from cluster port e1a on node1, and then connect e1a to port 1 on cluster switch cs1, using the appropriate cabling supported by the CN1610 switches.

    The Hardware Universe contains more information about cabling.

15. Disconnect the cable from cluster port e1a on node2, and then connect e1a to port 2 on cluster switch cs1, using the appropriate cabling supported by the CN1610 switches.
16. Enable all of the node-facing ports on cluster switch cs1.

    Show example

    The following example shows that ports 1 through 12 are enabled on switch cs1:

```
(cs1)# configure
(cs1)(Config)# interface 0/1-0/12
(cs1)(Interface 0/1-0/12)# no shutdown
(cs1)(Interface 0/1-0/12)# exit
(cs1)(Config)# exit
```

17. Enable the first cluster port e1a on each node:

```
network port modify
```

Show example

The following example shows how to enable the port e1a on node1 and node2:

```
cluster::*> network port modify -node node1 -port e1a -up-admin true
cluster::*> network port modify -node node2 -port e1a -up-admin true
```

18. Verify that all of the cluster ports are `up`:

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

Show example

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

```
cluster::*> network port show -ipspace Cluster
                                      Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link   MTU Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ---- ----- ----------- ----------
------------
node1
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000
node2
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

19. Revert clus1 (which was previously migrated) to e1a on both nodes:

```
network interface revert
```

Show example

The following example shows how to revert clus1 to the port e1a on node1 and node2:

```
cluster::*> network interface revert -vserver node1 -lif clus1
cluster::*> network interface revert -vserver node2 -lif clus1
```

ⓘ For release 8.3 and later, use the following command: `network interface revert -vserver Cluster -lif <nodename_clus<N>>`

20. Verify that all of the cluster LIFs are `up`, operational, and display as `true` in the "Is Home" column:

    `network interface show -vserver Cluster`

    Show example

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

```
cluster::*> network interface show -vserver Cluster
            Logical    Status     Network       Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask  Node          Port
Home
----------- ---------- ---------- ------------- -------------
------- ----
node1
            clus1      up/up    10.10.10.1/16   node1         e1a
true
            clus2      up/up    10.10.10.2/16   node1         e2a
true
node2
            clus1      up/up    10.10.11.1/16   node2         e1a
true
            clus2      up/up    10.10.11.2/16   node2         e2a
true

4 entries were displayed.
```

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

    `cluster show`

Show example

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

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

22. Migrate clus2 to port e1a on the console of each node:

    `network interface migrate`

    Show example

    The following example shows the process for migrating clus2 to port e1a on node1 and node2:

```
cluster::*> network interface migrate -vserver node1 -lif clus2
-source-node node1 -dest-node node1 -dest-port e1a
cluster::*> network interface migrate -vserver node2 -lif clus2
-source-node node2 -dest-node node2 -dest-port e1a
```

> ⓘ For release 8.3 and later, use the following command: `network interface migrate -vserver Cluster -lif node1_clus2 -dest-node node1 -dest-port e1a`

23. Verify that the migration took place:

    `network interface show -vserver Cluster`

Show example

The following example verifies that clus2 is migrated to port e1a on node1 and node2:

```
cluster::*> network interface show -vserver Cluster
            Logical    Status     Network       Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask  Node          Port
Home
----------- ---------- ---------- ------------- -------------
------- ----
node1
            clus1      up/up    10.10.10.1/16   node1         e1a
true
            clus2      up/up    10.10.10.2/16   node1         e1a
false
node2
            clus1      up/up    10.10.11.1/16   node2         e1a
true
            clus2      up/up    10.10.11.2/16   node2         e1a
false

4 entries were displayed.
```

24. Shut down cluster port e2a on both nodes:

    `network port modify`

Show example

The following example shows how to shut down the port e2a on node1 and node2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin
false
cluster::*> network port modify -node node2 -port e2a -up-admin
false
```

25. Verify the port status:

    `network port show`

Show example

The following example shows that port e2a is `down` on node1 and node2:

```
cluster::*> network port show -role cluster
                                         Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link   MTU Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ---- ----- ----------- ----------
------------
node1
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        down  9000  true/true  full/full
auto/10000
node2
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        down  9000  true/true  full/full
auto/10000

4 entries were displayed.
```

26. Disconnect the cable from cluster port e2a on node1, and then connect e2a to port 1 on cluster switch cs2, using the appropriate cabling supported by the CN1610 switches.
27. Disconnect the cable from cluster port e2a on node2, and then connect e2a to port 2 on cluster switch cs2, using the appropriate cabling supported by the CN1610 switches.
28. Enable all of the node-facing ports on cluster switch cs2.

Show example

The following example shows that ports 1 through 12 are enabled on switch cs2:

```
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# no shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

29. Enable the second cluster port e2a on each node.

Show example

The following example shows how to enable the port e2a on node1 and node2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

30. Verify that all of the cluster ports are `up`:

    `network port show -ipspace Cluster`

    Show example

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

```
cluster::*> network port show -ipspace Cluster
                                              Auto-Negot  Duplex     Speed
(Mbps)
Node   Port   Role         Link   MTU Admin/Oper  Admin/Oper
Admin/Oper
------ ------ ------------ ---- ----- ----------- ----------
------------
node1
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000
node2
       e1a    clus1        up    9000  true/true  full/full
auto/10000
       e2a    clus2        up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

31. Revert clus2 (which was previously migrated) to e2a on both nodes:

    `network interface revert`

Show example

The following example shows how to revert clus2 to the port e2a on node1 and node2:

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```

For release 8.3 and later, the commands are: `cluster::*> network interface revert -vserver Cluster -lif node1_clus2` and `cluster::*> network interface revert -vserver Cluster -lif node2_clus2`

Step 3: Complete the configuration

1. Verify that all of the interfaces display `true` in the "Is Home" column:

   `network interface show -vserver Cluster`

   Show example

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

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

             Logical    Status     Network            Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask       Node
Port    Home
------------ ---------- ---------- ------------------ -----------
------- ----
node1
             clus1      up/up      10.10.10.1/16      node1
e1a     true
             clus2      up/up      10.10.10.2/16      node1
e2a     true
node2
             clus1      up/up      10.10.11.1/16      node2
e1a     true
             clus2      up/up      10.10.11.2/16      node2
e2a     true
```

2. Ping the cluster ports to verify the cluster connectivity:

   `cluster ping-cluster local`

The command output shows connectivity between all of the cluster ports.

3. Verify that both nodes have two connections to each switch:

```
show isdp neighbors
```

Show example

The following example shows the appropriate results for both switches:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID              Intf         Holdtime  Capability   Platform
Port ID
---------------------- ------------ --------- ------------ ---------
------------
node1                  0/1          132       H            FAS3270
e1a
node2                  0/2          163       H            FAS3270
e1a
cs2                    0/13         11        S            CN1610
0/13
cs2                    0/14         11        S            CN1610
0/14
cs2                    0/15         11        S            CN1610
0/15
cs2                    0/16         11        S            CN1610
0/16

(cs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID              Intf         Holdtime  Capability   Platform
Port ID
---------------------- ------------ --------- ------------ ---------
------------
node1                  0/1          132       H            FAS3270
e2a
node2                  0/2          163       H            FAS3270
e2a
cs1                    0/13         11        S            CN1610
0/13
cs1                    0/14         11        S            CN1610
0/14
cs1                    0/15         11        S            CN1610
0/15
cs1                    0/16         11        S            CN1610
0/16
```

4. Display information about the devices in your configuration:

   `network device discovery show`

5. Disable the two-node switchless configuration settings on both nodes using the advanced privilege command:

   `network options detect-switchless modify`

   Show example

   The following example shows how to disable the switchless configuration settings:

   ```
   cluster::*> network options detect-switchless modify -enabled false
   ```

   For release 9.2 and later, skip this step since the configuration is automatically converted.

6. Verify that the settings are disabled:

   `network options detect-switchless-cluster show`

   Show example

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

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

   For release 9.2 and later, wait until `Enable Switchless Cluster` is set to false. This can take up to three minutes.

7. Configure clusters clus1 and clus2 to auto revert on each node and confirm.

   Show example

   ```
   cluster::*> network interface modify -vserver node1 -lif clus1 -auto
   -revert true
   cluster::*> network interface modify -vserver node1 -lif clus2 -auto
   -revert true
   cluster::*> network interface modify -vserver node2 -lif clus1 -auto
   -revert true
   cluster::*> network interface modify -vserver node2 -lif clus2 -auto
   -revert true
   ```

For release 8.3 and later, use the following command: `network interface modify -vserver Cluster -lif * -auto-revert true` to enable auto-revert on all nodes in the cluster.

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

   `cluster show`

   Show example

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

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

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

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

   Show example

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

10. Change the privilege level back to admin:

    `set -privilege admin`

Replace switches

Replace a NetApp CN1610 cluster switch

Follow these steps to replace a defective NetApp CN1610 switch in a cluster network. This is a non-disruptive procedure (NDU).

What you'll need

Before you perform the switch replacement, the following conditions must exist before you perform the switch replacement in the current environment and on the replacement switch for existing cluster and network infrastructure:

- The existing cluster must be verified as completely functional, with at least one fully connected cluster switch.

- All of the cluster ports must be **up**.
- All of the cluster logical interfaces (LIFs) must be up and must not have been migrated.
- The ONTAP cluster `ping-cluster -node node1` command must indicate that basic connectivity and larger than PMTU communication are successful on all of the paths.

About this task

You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.

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

- The names of the two CN1610 cluster switches are `cs1` and `cs2`.
- The name of the CN1610 switch that is to be replaced (the defective switch) is `old_cs1`.
- The name of the new CN1610 switch (the replacement switch) is `new_cs1`.
- The name of the partner switch that is not being replaced is `cs2`.

Steps

1. Confirm that the startup configuration file matches the running configuration file. You must save these files locally for use during the replacement.

   The configuration commands in the following example are for FASTPATH 1.2.0.7:

   Show example

   ```
   (old_cs1) >enable
   (old_cs1) #show running-config
   (old_cs1) #show startup-config
   ```

2. Create a copy of the running configuration file.

   The command in the following example is for FASTPATH 1.2.0.7:

   Show example

   ```
   (old_cs1) #show running-config filename.scr
   Config script created successfully.
   ```

ⓘ You can use any file name except `CN1610_CS_RCF_v1.2.scr`. The file name must have the **.scr** extension.

3. Save the running configuration file of the switch to an external host in preparation for the replacement.

Show example

```
(old_cs1) #copy nvram:script filename.scr
scp://<Username>@<remote_IP_address>/path_to_file/filename.scr
```

4. Verify that the switch and ONTAP versions match in the compatibility matrix. See the NetApp CN1601 and CN1610 Switches page for details.
5. From the Software Downloads page on the NetApp Support Site, select NetApp Cluster Switches to download the appropriate RCF and FASTPATH versions.
6. Set up a Trivial File Transfer Protocol (TFTP) server with the FASTPATH, RCF, and saved configuration `.scr` file for use with the new switch.
7. Connect the serial port (the RJ-45 connector labeled "IOIOI" on the right side of the switch) to an available host with terminal emulation.
8. On the host, set the serial terminal connection settings:
   a. 9600 baud
   b. 8 data bits
   c. 1 stop bit
   d. parity: none
   e. flow control: none
9. Connect the management port (the RJ-45 wrench port on the left side of the switch) to the same network where your TFTP server is located.
10. Prepare to connect to the network with the TFTP server.

    If you are using Dynamic Host Configuration Protocol (DHCP), you do not have to configure an IP address for the switch at this time. The service port is set to use DHCP by default. The network management port is set to none for the IPv4 and IPv6 protocol settings. If your wrench port is connected to a network that has a DHCP server, then the server settings are configured automatically.

    To set a static IP address, you should use the serviceport protocol, network protocol, and serviceport ip commands.

    Show example

```
(new_cs1) #serviceport ip <ipaddr> <netmask> <gateway>
```

11. Optionally, if the TFTP server is on a laptop, then connect the CN1610 switch to the laptop by using a standard Ethernet cable, and then configure its network port in the same network with an alternate IP address.

    You can use the `ping` command to verify the address. If you are unable to establish the connectivity, you should use a nonrouted network, and configure the service port using IP 192.168.x or 172.16.x. You can reconfigure the service port to the production management IP address at a later date.

12. Optionally, verify and install the appropriate versions of the RCF and FASTPATH software for the new switch. If you have verified that the new switch is correctly set up and does not require updates to the RCF and FASTPATH software, you should go to step 13.

    a. Verify the new switch settings.

    Show example

    ```
    (new_cs1) >*enable*
    (new_cs1) #show version
    ```

    b. Download the RCF to the new switch.

    Show example

    ```
    (new_cs1) #copy tftp://<server_ip_address>/CN1610_CS_RCF_v1.2.txt
    nvram:script CN1610_CS_RCF_v1.2.scr
    Mode.   TFTP
    Set Server IP.  172.22.201.50
    Path.   /
    Filename.......................................
    CN1610_CS_RCF_v1.2.txt
    Data Type...................................... Config Script
    Destination Filename...........................
    CN1610_CS_RCF_v1.2.scr
    File with same name already exists.
    WARNING:Continuing with this command will overwrite the existing
    file.

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

    File transfer in progress. Management access will be blocked for
    the duration of the transfer. please wait...
    Validating configuration script...
    (the entire script is displayed line by line)
    ...
    description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
    ...
    Configuration script validated.
    File transfer operation completed successfully.
    ```

    c. Verify that the RCF is downloaded to the switch.

Show example

```
(new_cs1) #script list
Configuration Script Nam   Size(Bytes)
-------------------------- -----------
CN1610_CS_RCF_v1.1.scr            2191
CN1610_CS_RCF_v1.2.scr            2240
latest_config.scr                 2356

4 configuration script(s) found.
2039 Kbytes free.
```

13. Apply the RCF to the CN1610 switch.

Show example

```
(new_cs1) #script apply CN1610_CS_RCF_v1.2.scr
Are you sure you want to apply the configuration script? (y/n) y
...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script 'CN1610_CS_RCF_v1.2.scr' applied. Note that the
script output will go to the console.
After the script is applied, those settings will be active in the
running-config file. To save them to the startup-config file, you
must use the write memory command, or if you used the reload answer
yes when asked if you want to save the changes.
```

a. Save the running configuration file so that it becomes the startup configuration file when you reboot the switch.

Show example

```
(new_cs1) #write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.

Configuration Saved!
```

b. Download the image to the CN1610 switch.

Show example

```
(new_cs1) #copy
tftp://<server_ip_address>/NetApp_CN1610_1.2.0.7.stk active
Mode.   TFTP
Set Server IP.  tftp_server_ip_address
Path.   /
Filename......................................
NetApp_CN1610_1.2.0.7.stk
Data Type.  Code
Destination Filename.   active

Management access will be blocked for the duration of the
transfer

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

TFTP Code transfer starting...

File transfer operation completed successfully.
```

c. Run the new active boot image by rebooting the switch.

The switch must be rebooted for the command in step 6 to reflect the new image. There are two possible views for a response that you might see after you enter the reload command.

Show example

```
(new_cs1) #reload
The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved! System will now restart!
.
.
.
Cluster Interconnect Infrastructure

User:admin Password: (new_cs1) >*enable*
```

d. Copy the saved configuration file from the old switch to the new switch.

Show example

```
(new_cs1) #copy tftp://<server_ip_address>/<filename>.scr
nvram:script <filename>.scr
```

e. Apply the previously saved configuration to the new switch.

Show example

```
(new_cs1) #script apply <filename>.scr
Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

f. Save the running configuration file to the startup configuration file.

Show example

```
(new_cs1) #write memory
```

14. 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.

15. On the new switch new_cs1, log in as the admin user, and shut down all of the ports that are connected to the node cluster interfaces (ports 1 through 12).

    Show example

    ```
    User:*admin*
    Password:
    (new_cs1) >*enable*
    (new_cs1) #

    (new_cs1) config
    (new_cs1)(config)interface 0/1-0/12
    (new_cs1)(interface 0/1-0/12)shutdown
    (new_cs1)(interface 0/1-0/12)exit
    (new_cs1) #write memory
    ```

16. Migrate the cluster LIFs from the ports that are connected to the old_cs1 switch.

    You must migrate each cluster LIF from its current node's management interface.

    Show example

    ```
    cluster::> set -privilege advanced
    cluster::> network interface migrate -vserver <vserver_name> -lif
    <Cluster_LIF_to_be_moved> - sourcenode <current_node> -dest-node
    <current_node> -dest-port <cluster_port_that_is_UP>
    ```

17. Verify that all of the cluster LIFs have been moved to the appropriate cluster port on each node.

Show example

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

18. Shut down the cluster ports that are attached to the switch that you replaced.

Show example

```
cluster::*> network port modify -node <node_name> -port
<port_to_admin_down> -up-admin false
```

19. Verify the health of the cluster.

Show example

```
cluster::*> cluster show
```

20. Verify that the ports are down.

Show example

```
cluster::*> cluster ping-cluster -node <node_name>
```

21. On the switch cs2, shut down the ISL ports 13 through 16.

Show example

```
(cs2) config
(cs2)(config)interface 0/13-0/16
(cs2)(interface 0/13-0/16)#shutdown
(cs2) #show port-channel 3/1
```

22. Verify whether the storage administrator is ready for the replacement of the switch.
23. Remove all of the cables from the old_cs1 switch, and then connect the cables to the same ports on the new_cs1 switch.
24. On the cs2 switch, bring up the ISL ports 13 through 16.

Show example

```
(cs2) config
(cs2)(config)interface 0/13-0/16
(cs2)(interface 0/13-0/16)#no shutdown
```

25. Bring up the ports on the new switch that are associated with the cluster nodes.

Show example

```
(cs2) config
(cs2)(config)interface 0/1-0/12
(cs2)(interface 0/13-0/16)#no shutdown
```

26. On a single node, bring up the cluster node port that is connected to the replaced switch, and then confirm that the link is up.

Show example

```
cluster::*> network port modify -node node1 -port
<port_to_be_onlined> -up-admin true
cluster::*> network port show -role cluster
```

27. Revert the cluster LIFs that are associated with the port in step 25 on the same node.

In this example, the LIFs on node1 are successfully reverted if the “Is Home” column is true.

Show example

```
cluster::*> network interface revert -vserver node1 -lif
<cluster_lif_to_be_reverted>
cluster::*> network interface show -role cluster
```

28. If the first node’s cluster LIF is up and is reverted to its home port, repeat steps 25 and 26 to bring up the cluster ports and to revert the cluster LIFs on the other nodes in the cluster.
29. Display information about the nodes in the cluster.

Show example

```
cluster::*> cluster show
```

30. Confirm that the startup configuration file and running configuration file are correct on the replaced switch. This configuration file should match the output in step 1.

Show example

```
(new_cs1) >*enable*
(new_cs1) #show running-config
(new_cs1) #show startup-config
```

31. 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 NetApp CN1610 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.

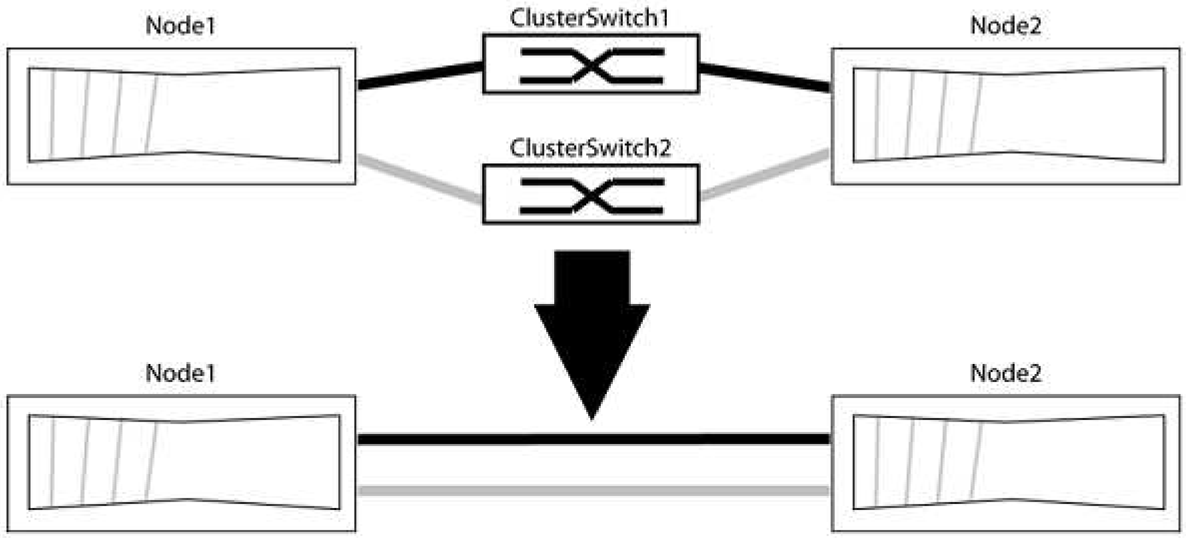
What you'll need

- 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

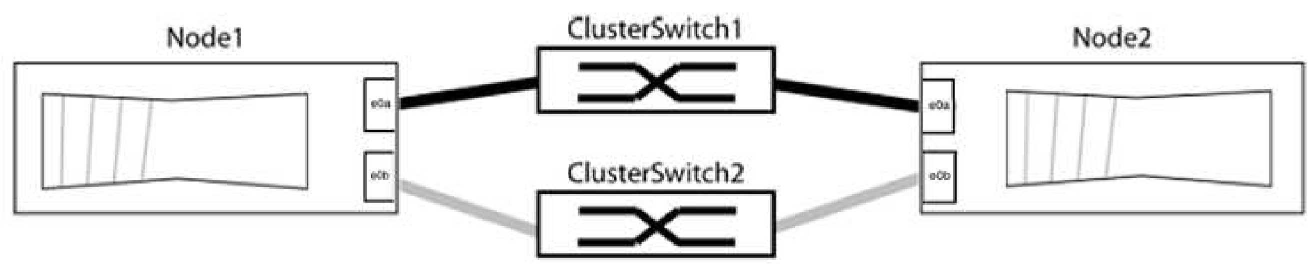
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

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
   ```

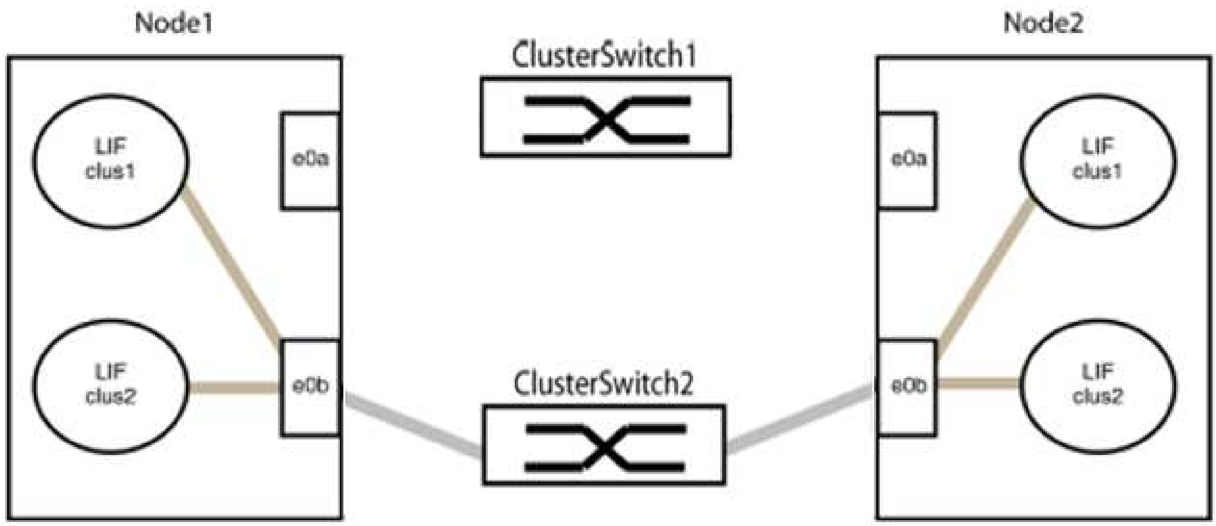
   All units must be either master or secondary.

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**.

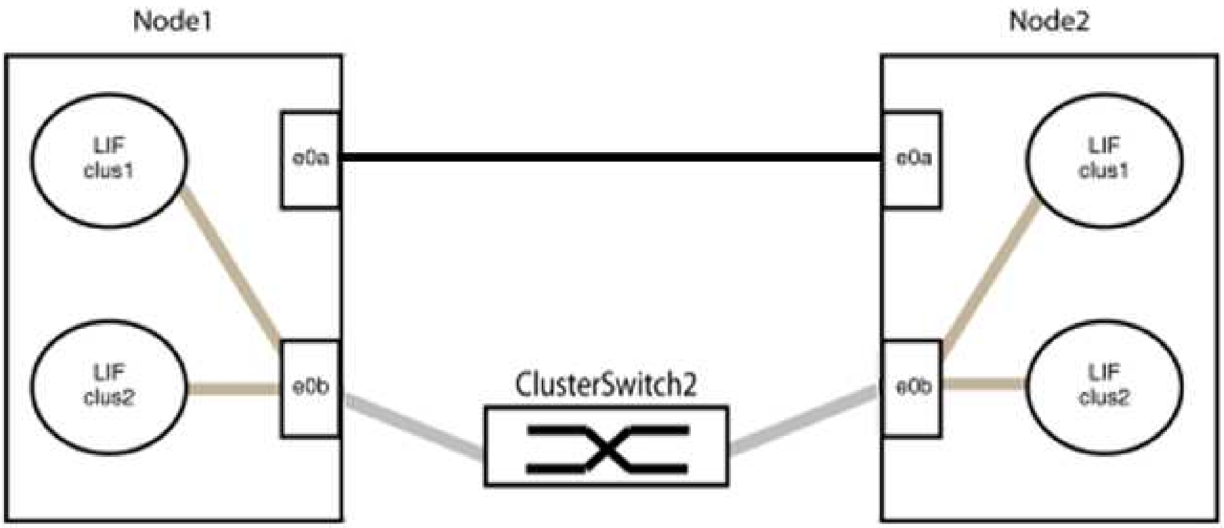
   a. Disconnect all the cables from the ports in group1 at the same time.

      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:



9. The switchless cluster network option transitions from `false` to `true`. This might take up to 45 seconds. Confirm that the switchless option is set to `true`:

   `network options switchless-cluster show`

   The following example shows that the switchless cluster is enabled:

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

10. Verify that the cluster network is not disrupted:

    `cluster ping-cluster -node local`

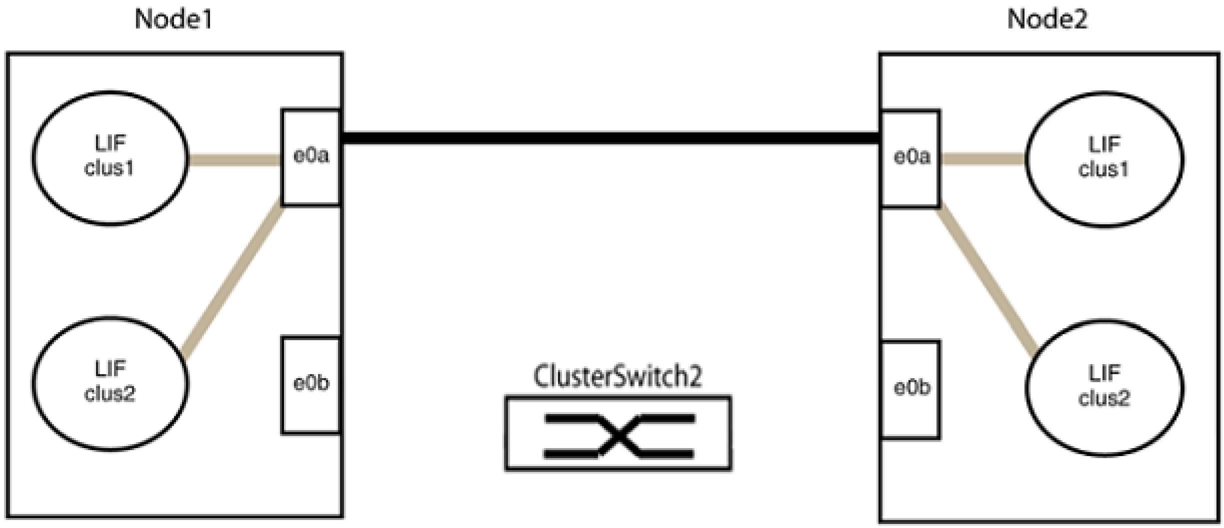
    > Before proceeding to the next step, you must wait at least two minutes to confirm a working back-to-back connection on group 1.

11. Set up the switchless configuration for the ports in group 2.

    > To avoid potential networking issues, you must disconnect the ports from group2 and reconnect them back-to-back as quickly as possible, for example, **in less than 20 seconds**.

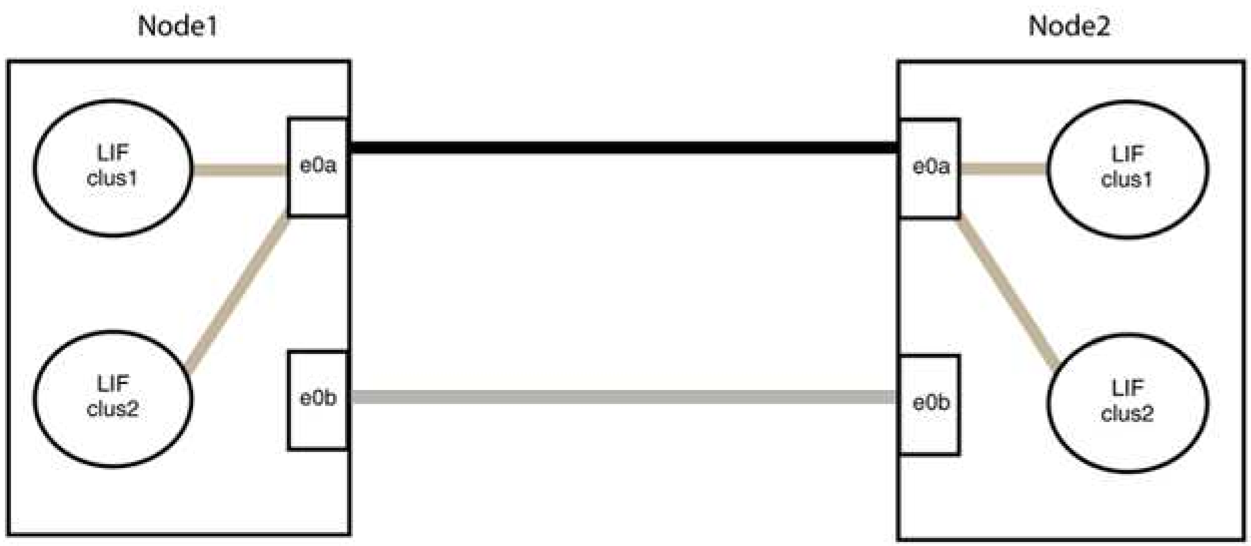
    a. Disconnect all the cables from the ports in group2 at the same time.

       In the following example, the cables are disconnected from port "e0b" on each node, and cluster traffic continues through the direct connection between the "e0a" ports:



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

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



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
```