



Cisco Nexus 9336C-FX2 switches

Cluster and storage switches

NetApp

October 14, 2022

Table of Contents

- Cisco Nexus 9336C-FX2 switches 1
 - Cisco 9336C-FX2 switch overview 1
 - Install a Cisco Nexus 9336C-FX2 switch and pass-through panel in a NetApp cabinet 2
 - Set up 6
 - Install NX-OS software and RCFs on Cisco Nexus 9336C-FX2 cluster switches 34
 - Migrate from a Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch 63
 - Migrate to a two-node switched cluster with Cisco Nexus 9336C-FX2 cluster switches 81
 - Configure a Cisco Nexus 9336C-FX2 cluster switch 95
 - Replace a Cisco Nexus 9336C-FX2 cluster switch 124
 - Replace a Cisco Nexus 9336C-FX2 storage switch 138

Cisco Nexus 9336C-FX2 switches

Cisco 9336C-FX2 switch overview

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

You can install the Cisco Nexus 9336C-FX2 switch (X190200/X190210) in a NetApp system cabinet or third-party cabinet with the standard brackets that are included with the switch.

The following table lists the part number and description for the 9336C-FX2 switch, fans, and power supplies:

Part number	Description
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT10/25/40/100GQSFP28
X190002	Accessory Kit X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100W PSU - Port side exhaust airflow
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100W PSU - Port side Intake airflow
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, Port side exhaust airflow
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, Port side intake airflow

Other supported switches

- Nexus 3232C

You can install the Cisco Nexus 3232C switch (X190100) NetApp system cabinet with the custom brackets that come with the switch, or you can install it in a rack with the standard brackets that are also included with the switch.

- Nexus 3132Q-V

You can install the Cisco Nexus 3132Q-V switch (X190001) in a NetApp system cabinet or third-party cabinet with the standard brackets that are included with the switch.

The following cluster switches are no longer available from NetApp, but will be supported by Cisco for a limited time:

- Nexus 5596UP/5596T

You can install the Cisco Nexus 5596UP switch (X1967-R6) or 5596T (X1989-R6) in a NetApp system cabinet with the custom brackets that come with the switch, or you can install it in a rack with the standard brackets that are also included with the switch.

The Nexus 5596UP switch also supports one or two 16-port expansion modules (X1988-R6).

The Nexus 5596T switch is only supported as a cluster interconnect switch for the FAS2520 and is intended to be used for performing nondisruptive hardware upgrades.

[End of Availability](#) details.

Install a Cisco Nexus 9336C-FX2 switch and pass-through panel in a NetApp cabinet

You can install the Cisco Nexus 9336C-FX2 switch and pass-through panel in a NetApp cabinet with the standard brackets that are included with the switch.

About this task

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

[Cisco Nexus 9000 Series Hardware Installation Guide](#)

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



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

Steps

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

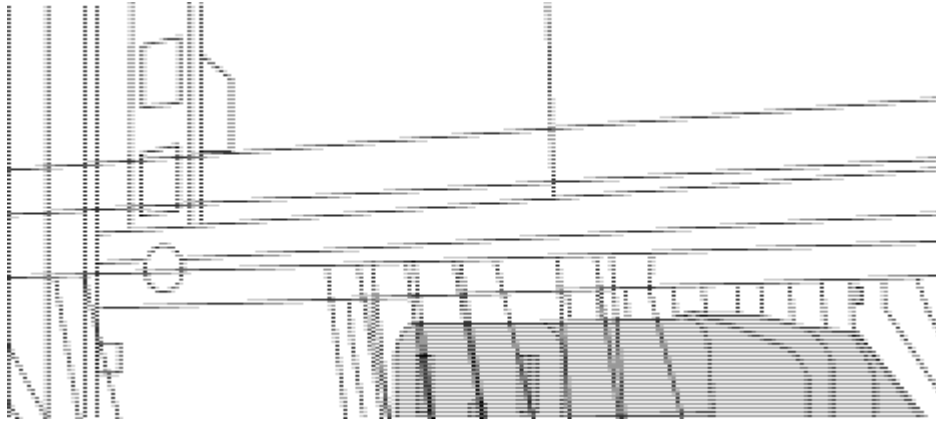
The pass-through panel kit is available from NetApp (part number X8784-R6).

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

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

In this procedure, the blanking panel will be installed in U40.
 - b. Install two clip nuts on each side in the appropriate square holes for front cabinet rails.
 - c. Center the panel vertically to prevent intrusion into adjacent rack space, and then tighten the screws.

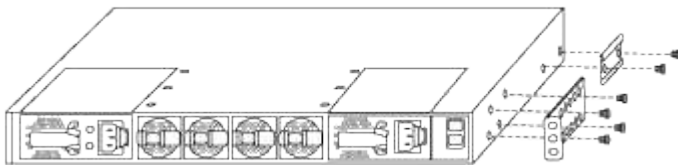
- d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



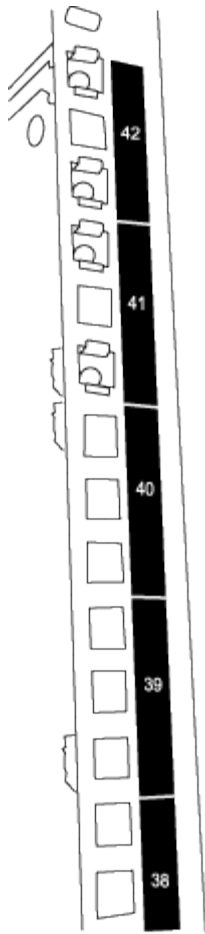
- i. Female connector of the jumper cord.

2. Install the rack-mount brackets on the Nexus 9336C-FX2 switch chassis.

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



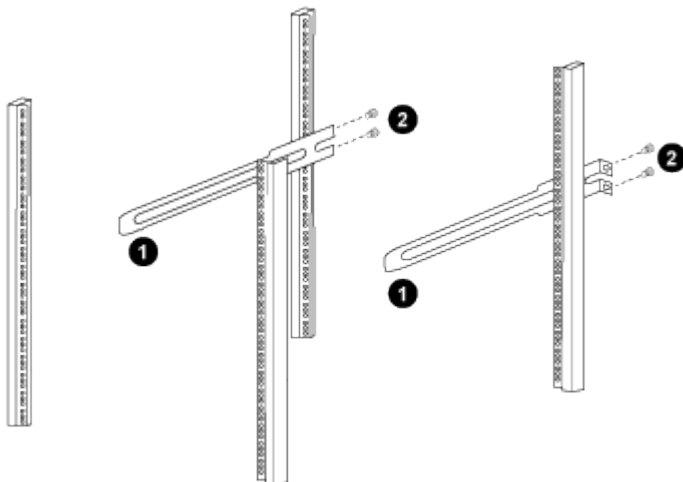
- b. Repeat step [2a](#) with the other front rack-mount bracket on the other side of the switch.
 - c. Install the rear rack-mount bracket on the switch chassis.
 - d. Repeat step [2c](#) with the other rear rack-mount bracket on the other side of the switch.
3. Install the clip nuts in the square hole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



The two 9336C-FX2 switches will always be mounted in the top 2U of the cabinet RU41 and 42.

4. Install the slider rails in the cabinet.

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



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

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

5. Install the switch in the cabinet.



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

a. Position the back of the switch at RU41.



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

ii. Gently slide the switch until the front rack-mount brackets are flush with the front posts.

b. Attach the switch to the cabinet.



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

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

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



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

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



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

8. Connect the management port on each 9336C-FX2 switch to either of the management switches (if ordered) or connect them directly to your management network.

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

Set up

Set up the switches

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

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

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

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

[NetApp documentation](#)

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



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



For more information refer to the [Hardware Universe](#).

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



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

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

Steps

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

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

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

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

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

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

Related information

[Required cluster configuration information](#)

[Required documentation](#)

[Sample and blank cabling worksheets](#)

Required cluster configuration information

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

Required network information for all switches

You need the following network information for all switch configurations:

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

Refer to the [Hardware Universe](#) for latest information.

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

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

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

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

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

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

- Enter the password for admin:

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

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

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

- Create another login account? (yes/no)

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

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

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

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

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

- Enter the switch name.

The switch name is limited to 63 alphanumeric characters.

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

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

- Configure the default-gateway? (yes/no)

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

- Configure advanced IP options? (yes/no)

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

- Enable the telnet service? (yes/no)

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

- Enabled SSH service? (yes/no)

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



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

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

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

- Configure default interface layer (L3/L2):

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

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

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

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

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

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

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

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

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

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



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

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

[Cisco Nexus 9336C-FX2 Installation and Upgrade Guides](#)

[Cisco Nexus 92300YC Installation and Upgrade Guides](#)

[Cisco Nexus 5000 Series Hardware Installation Guide](#)

[Cisco Nexus 3000 Series Hardware Installation Guide](#)

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

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

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



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

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

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

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

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

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

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

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

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

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



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

Required documentation

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

Required documentation for cluster network switches

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

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

Document title	Description
<i>Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide</i> (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
<i>Cisco Nexus 9000 Series NX-OS Command Reference Master Index</i>	Provides links to the various command references provided by Cisco.
<i>Cisco Nexus 9000 MIBs Reference</i>	Describes the Management Information Base (MIB) files for the Nexus 9000 switches.
<i>Nexus 9000 Series NX-OS System Message Reference</i>	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.
<i>Cisco Nexus 9000 Series NX-OS Release Notes</i> (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 9000 Series.
Regulatory Compliance and Safety Information for Cisco Nexus 9000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 9000 series switches.

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

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

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

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

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

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

Required documentation for supported ONTAP systems

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

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

Rail kit and cabinet documentation

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

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

Considerations for using Smart Call Home

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

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

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

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

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

[Cisco support site](#)

Sample and blank cabling worksheets

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

Cisco Nexus 9336C-FX2 cabling worksheet

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

Sample cabling worksheet

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

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

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

Blank cabling worksheet

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

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

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

Cisco Nexus 92300YC cabling worksheet

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

Sample cabling worksheet

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

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

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

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

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

Blank cabling worksheet

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

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

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

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

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

Cisco Nexus 3232C cabling worksheet

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

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

Sample cabling worksheet

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

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

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

Blank cabling worksheet

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

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

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

Cisco Nexus 3132Q-V cabling worksheet

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

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

Sample cabling worksheet

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

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

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

Blank cabling worksheet

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

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

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

Cisco Nexus 5596UP and 5596T cabling worksheet

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

Sample cabling worksheet

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

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

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

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

Blank cabling worksheet

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



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

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

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

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

Install NX-OS software and RCFs on Cisco Nexus 9336C-FX2 cluster switches

Install NX-OS software and RCFs on Cisco Nexus 9336C-FX2 cluster switches

The Cisco NX-OS software and reference configuration files (RCFs) must be installed on Cisco Nexus 9336C-FX2 cluster switches.

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

- The cluster must be fully functioning (there should be no errors in the logs or similar issues).
- You must have checked or set your desired boot configuration in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.
- If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- You must have a console connection to the switch, required when installing the RCF.
- You must have consulted the switch compatibility table on the [Cisco Ethernet switch](#) page for the supported ONTAP, NX-OS, and RCF versions.
- There can be command dependencies between the command syntax in the RCF and that found in versions of NX-OS.
- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures on **Cisco Nexus 9000**

Series Switches.

Cisco Nexus 9000 Series Switches

- You must have the current RCF.



Before installing a new switch software version and RCFs, you must erase the switch settings and perform basic configuration. You must be connected to the switch using the serial console. This task resets the configuration of the management network.

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

See the [Hardware Universe](#) to verify the correct cluster ports on your platforms.



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

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

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



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

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=x h`

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



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

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

```
set -privilege advanced
```

The advanced prompt (`*>`) appears.

3. Display how many cluster interconnect interfaces are configured in each node for each cluster interconnect switch: `network device-discovery show -protocol cdp`

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

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

4 entries were displayed.

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

a. Display the network port attributes: `network port show -ipspace Cluster`

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

Node: cluster1-02

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

Node: cluster1-01

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

4 entries were displayed.

b. Display information about the LIFs: `network interface show -vserver Cluster`

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.209.69/16	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.49.125/16	
cluster1-01	e0b true			
	cluster1-02_clus1	up/up	169.254.47.194/16	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.19.183/16	
cluster1-02	e0b true			

4 entries were displayed.

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

```

cluster1::*> cluster ping-cluster -node cluster1-02
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

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

```

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

```

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

4 entries were displayed.

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


```

cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>

```



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

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

```

cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>

```



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

Install the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 9336C-FX2 cluster switch.

Steps

1. Connect the cluster switch to the management network.

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

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

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

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

3. Copy the NX-OS software and EPLD images to the Nexus 9336C-FX2 switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management

Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
but not
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.38
  NXOS: version 9.3(4)
  BIOS compile time: 05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]

Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash: 53298520 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)

  Last reset at 157524 usecs after Mon Nov 2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

5. Install the NX-OS image.

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

```
cs2# install all nxos bootflash:nxos.9.3.5.bin
```

```
Installer will perform compatibility check first. Please wait.
```

```
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
```

```
[#####] 100% -- SUCCESS
```

```
Verifying image type.
```

```
[#####] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
```

```
[#####] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
```

```
[#####] 100% -- SUCCESS
```

```
Performing module support checks.
```

```
[#####] 100% -- SUCCESS
```

```
Notifying services about system upgrade.
```

```
[#####] 100% -- SUCCESS
```

```
Compatibility check is done:
```

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

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt	New-Version
Upg-Required			
1	nxos	9.3(4)	9.3(5)
yes			
1	bios	v08.37(01/28/2020):v08.23(09/23/2015)	
v08.38(05/29/2020)		yes	

Switch will be reloaded for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

Performing runtime checks.

[#####] 100% -- SUCCESS

Setting boot variables.

[#####] 100% -- SUCCESS

Performing configuration copy.

[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.

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

```
cs2# show version
```

Cisco Nexus Operating System (NX-OS) Software

TAC support: <http://www.cisco.com/tac>

Copyright (C) 2002-2020, Cisco and/or its affiliates.

All rights reserved.

The copyrights to certain works contained in this software are owned by other third parties and used and distributed under their own licenses, such as open source. This software is provided "as is," and

unless
otherwise stated, there is no warranty, express or implied, including
but not
limited to warranties of merchantability and fitness for a particular
purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
<http://www.opensource.org/licenses/gpl-2.0.php> and
<http://opensource.org/licenses/gpl-3.0.html> and
<http://www.opensource.org/licenses/lgpl-2.1.php> and
<http://www.gnu.org/licenses/old-licenses/library.txt>.

Software

BIOS: version 05.33
NXOS: version 9.3(5)
BIOS compile time: 09/08/2018
NXOS image file is: bootflash:///nxos.9.3.5.bin
NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]

Hardware

cisco Nexus9000 C9336C-FX2 Chassis
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
Processor Board ID FOC20291J6K

Device name: cs2
bootflash: 53298520 kB

Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)

Last reset at 277524 usecs after Mon Nov 2 22:45:12 2020

Reason: Reset due to upgrade
System version: 9.3(4)
Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

7. Upgrade the EPLD image and reboot the switch.

```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

8. After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x19
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 9336C-FX2 switch for the first time. You can also use this procedure to upgrade your RCF version.

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

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



- The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.
- Before you perform this procedure make sure that you have a current backup of the switch configuration.

Steps

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

```

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

```

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

- Verify that all the cluster ports are up with a healthy status: `network port show -role cluster`

```

cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore

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

```

Node: cluster1-02

Ignore

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

8 entries were displayed.

Node: cluster1-03

Ignore

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

Node: cluster1-04

Ignore

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

cluster1::*>

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

cluster

```
cluster1::*> network interface show -role cluster
```

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

Cluster					
01	e0a	cluster1-01_clus1 true	up/up	169.254.3.4/23	cluster1-
01	e0d	cluster1-01_clus2 true	up/up	169.254.3.5/23	cluster1-
02	e0a	cluster1-02_clus1 true	up/up	169.254.3.8/23	cluster1-
02	e0d	cluster1-02_clus2 true	up/up	169.254.3.9/23	cluster1-
03	e0a	cluster1-03_clus1 true	up/up	169.254.1.3/23	cluster1-
03	e0b	cluster1-03_clus2 true	up/up	169.254.1.1/23	cluster1-
04	e0a	cluster1-04_clus1 true	up/up	169.254.1.6/23	cluster1-
04	e0b	cluster1-04_clus2 true	up/up	169.254.1.7/23	cluster1-

8 entries were displayed.
cluster1::*>

- c. Verify that the cluster displays information for both cluster switches: `system cluster-switch show -is-monitoring-enabled-operational true`

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
```

Switch	Type	Address	Model
cs1	cluster-network	10.233.205.90	N9K-C9336C
Serial Number: FOCXXXXXXGD Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5) Version Source: CDP			
cs2	cluster-network	10.233.205.91	N9K-C9336C
Serial Number: FOCXXXXXXGS Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5) Version Source: CDP			

```
cluster1::*>
```

3. Disable auto-revert on the cluster LIFs.

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

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

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

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

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

```
cluster1::*> network interface show -role cluster
```

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0a	true			
	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0a	false			
	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0a	true			
	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0a	false			
	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0a	true			
	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0a	false			
	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0a	true			
	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04
e0a	false			

8 entries were displayed.
cluster1::*>

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

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

4 entries were displayed.
cluster1::*>

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

```
show running-config
```

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



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

a. Clean the configuration. This step requires a console connection to the switch.

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

b. Perform a basic setup of the switch.

9. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 9000 Series NX-OS Command Reference](#) guides.

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

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

10. Apply the RCF previously downloaded to the bootflash.

For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 9000 Series NX-OS Command Reference](#) guides.

This example shows the RCF file `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` being installed on switch cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
```

11. Examine the banner output from the `show banner motd` command. You must read and follow these instructions to ensure the proper configuration and operation of the switch.

```
cs2# show banner motd
```

```
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Nexus N9K-C9336C-FX2
* Filename  : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date      : 10-23-2020
* Version   : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int e1/1/1-4,
e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int e1/4/1-
4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G configuration
in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

12. Verify that the RCF file is the correct newer version: `show running-config`

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

- The RCF banner

- The node and port settings
- Customizations The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.

13. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file.

For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 9000 Series NX-OS Command Reference](#) guides.

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

14. Reboot switch cs2. You can ignore the “cluster ports down” events reported on the nodes while the switch reboots.

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

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

- Verify that e0d ports are up and healthy across all nodes in the cluster: `network port show -role cluster`

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

Node: cluster1-01

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

Node: cluster1-02

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

```

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

Node: cluster1-03

Ignore

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

Node: cluster1-04

Ignore

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

```

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

```

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

```

```

cluster1-01/cdp
    e0a    cs1                                Ethernet1/7    N9K-
C9336C
    e0d    cs2                                Ethernet1/7    N9K-
C9336C
cluster01-2/cdp
    e0a    cs1                                Ethernet1/8    N9K-
C9336C
    e0d    cs2                                Ethernet1/8    N9K-
C9336C
cluster01-3/cdp
    e0a    cs1                                Ethernet1/1/1  N9K-
C9336C
    e0b    cs2                                Ethernet1/1/1  N9K-
C9336C
cluster1-04/cdp
    e0a    cs1                                Ethernet1/1/2  N9K-
C9336C
    e0b    cs2                                Ethernet1/1/2  N9K-
C9336C

```

```

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true

```

Switch	Type	Address	Model
cs1	cluster-network	10.233.205.90	NX9-

C9336C

Serial Number: FOCXXXXXXGD

Is Monitored: true

Reason: None

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

9.3(5)

Version Source: CDP

cs2	cluster-network	10.233.205.91	NX9-
-----	-----------------	---------------	------

C9336C

Serial Number: FOCXXXXXXGS

Is Monitored: true

Reason: None

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

9.3(5)

Version Source: CDP

2 entries were displayed.



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

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER: Blocking
port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL: Blocking
port-channel1 on VLAN0092. Inconsistent local vlan.
```

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

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

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

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

```

cluster1::*> network interface show -role cluster

```

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	false			
	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	true			
	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	false			
	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0d	true			
	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0b	false			
	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0b	true			
	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0b	false			
	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04
e0b	true			

```

8 entries were displayed.
cluster1::*>

```

18. Verify that the cluster is healthy: cluster show

```

cluster1::*> cluster show

```

Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

```

4 entries were displayed.
cluster1::*>

```

19. Repeat Steps 7 to 14 on switch cs1.

20. Enable auto-revert on the cluster LIFs.

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

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

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

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

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

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

```
cs1# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lACP mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports      Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

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

```

cluster1::*> network interface show -role cluster

```

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

Cluster				
e0d	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0b	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0b	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0b	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0b	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04

```

8 entries were displayed.
cluster1::*>

```

25. Verify that the cluster is healthy: cluster show

```

cluster1::*> cluster show

```

Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

```

4 entries were displayed.
cluster1::*>

```

26. Ping the remote cluster interfaces to verify connectivity: cluster ping-cluster -node local


```

cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)

```

Migrate from a Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch

Migrate from an older Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch

You must be aware of certain configuration information, port connections and cabling

requirements when you are replacing some older Cisco Nexus cluster switches with Cisco Nexus 9336C-FX2 cluster switches.

- The following cluster switches are supported:
 - Nexus 9336C-FX2
 - Nexus 5596UP
 - Nexus 3232C
 - Nexus 3132Q-V
- See the [Hardware Universe](#) for full details of supported ports and their configurations.
- You have configured some of the ports on Nexus 9336C-FX2 switches to run at 10 GbE or 40 GbE.
- You have planned, migrated, and documented 10 GbE and 40 GbE connectivity from nodes to Nexus 9336C-FX2 cluster switches.
- The ONTAP and NX-OS versions supported in this procedure are on the [Cisco Ethernet Switches](#) page.

How to migrate from an older Cisco switch to a Cisco Nexus 9336C-FX2 cluster switch

You can migrate nondisruptively older Cisco cluster switches for an ONTAP cluster to Cisco Nexus 9336C-FX2 cluster network switches.

Before you begin

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

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

About this task

The examples in this procedure use two nodes. These nodes use two 10GbE cluster interconnect ports e0a and e0b. See the [Hardware Universe](#) to verify the correct cluster ports on your platforms.



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

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

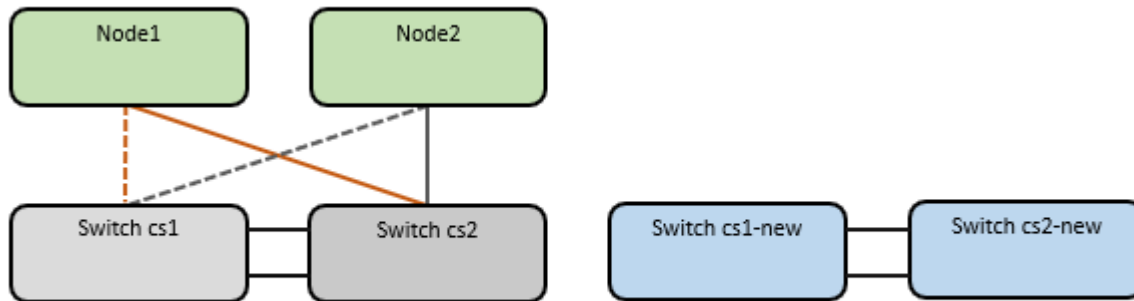
- The names of the existing two Cisco switches are **cs1** and **cs2**

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



The procedure requires the use of both ONTAP commands and [Nexus 9000 Series Switches](#) commands; ONTAP commands are used, unless otherwise indicated.

Initial switch setup



Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=xh`

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



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

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

The advanced prompt (***>**) appears.

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

```
cs1-new# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
```

```
-----
-----
1      Pol(SU)       Eth       LACP      Eth1/35(P)  Eth1/36(P)
```

```
cs2-new# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
```

```
-----
-----
1      Pol(SU)       Eth       LACP      Eth1/35(P)  Eth1/36(P)
```

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

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node1	/cdp			
	e0a	cs1	Ethernet1/1	N5K-
C5596UP				
	e0b	cs2	Ethernet1/2	N5K-
C5596UP				
node2	/cdp			
	e0a	cs1	Ethernet1/1	N5K-
C5596UP				
	e0b	cs2	Ethernet1/2	N5K-
C5596UP				

5. Determine the administrative or operational status for each cluster port.

- Verify that all the cluster ports are up with a healthy status: `network port show -ip space Cluster`

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

```
Node: node1
```

```
Ignore
```

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

```
Node: node2
```

```
Ignore
```

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

- b. Verify that all the cluster interfaces (LIFs) are on their home ports: `network interface show -vserver Cluster`

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

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
e0a	node1_clus1	up/up	169.254.209.69/16	node1
e0b	node1_clus2	up/up	169.254.49.125/16	node1
e0a	node2_clus1	up/up	169.254.47.194/16	node2
e0b	node2_clus2	up/up	169.254.19.183/16	node2
e0a	true			
e0b	true			

- c. Verify that the cluster displays information for both cluster switches: `system cluster-switch show -is-monitoring-enabled-operational true`

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
```

Switch	Type	Address	Model
cs1	cluster-network	10.233.205.92	N5K-C5596UP
Serial Number: FOXXXXXXXXGS Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(4) Version Source: CDP			
cs2	cluster-network	10.233.205.93	N5K-C5596UP
Serial Number: FOXXXXXXXXGD Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(4) Version Source: CDP			

6. Disable auto-revert on the cluster LIFs.

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

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

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

8. Verify that the cluster LIFs have migrated to the ports hosted on cluster switch cs1. This might take a few seconds: `network interface show -vserver Cluster`


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

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
Cluster					
true	node1_clus1	up/up	169.254.3.4/16	node1	e0a
false	node1_clus2	up/up	169.254.3.5/16	node1	e0a
true	node2_clus1	up/up	169.254.3.8/16	node2	e0a
false	node2_clus2	up/up	169.254.3.9/16	node2	e0a

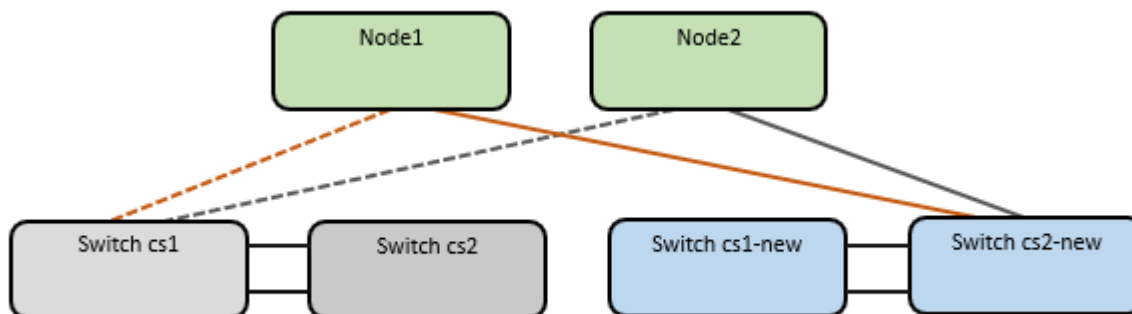
9. Verify that the cluster is healthy: `cluster show`

```
cluster1::*> cluster show
```

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

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

Cluster node connections moved to the cs2-new switch



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

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

```
Node: node1
```

```
Ignore
```

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

```
Node: node2
```

```
Ignore
```

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

All cluster ports that were moved should be up.

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

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node1	/cdp			
	e0a	cs1	Ethernet1/1	N5K-C5596UP
	e0b	cs2-new	Ethernet1/1/1	N9K-C9336C-
FX2				
node2	/cdp			
	e0a	cs1	Ethernet1/2	N5K-C5596UP
	e0b	cs2-new	Ethernet1/1/2	N9K-C9336C-
FX2				

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

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

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

14. On cluster switch cs1, shut down the ports connected to the cluster ports of the nodes. The following example uses the interface example output from step 7.

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

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

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

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interfac	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
Cluster					
false	node1_clus1	up/up	169.254.3.4/16	node1	e0b
true	node1_clus2	up/up	169.254.3.5/16	node1	e0b
false	node2_clus1	up/up	169.254.3.8/16	node2	e0b
true	node2_clus2	up/up	169.254.3.9/16	node2	e0b

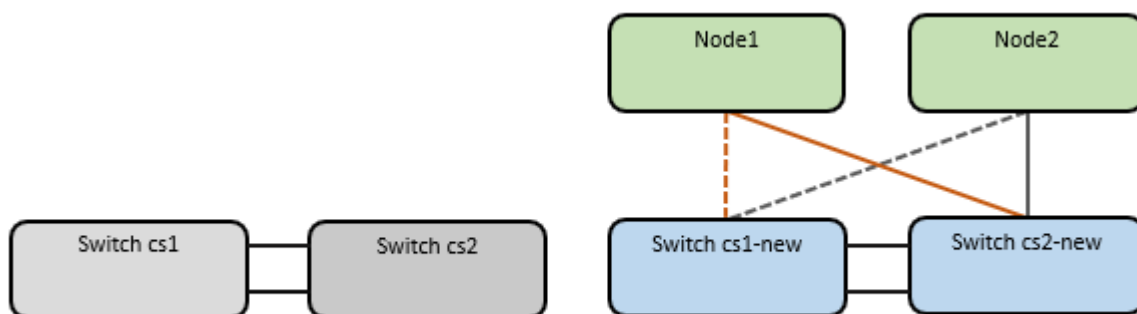
16. Verify that the cluster is healthy: `cluster show`

```
cluster1::*> cluster show
```

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

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

Cluster node connections moved to the cs1-new switch



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

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

```
Node: node1
```

```
Ignore
```

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

```
Node: node2
```

```
Ignore
```

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

All cluster ports that were moved should be up.

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

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node1	/cdp			
	e0a	cs1-new	Ethernet1/1/1	N9K-C9336C-
FX2				
	e0b	cs2-new	Ethernet1/1/2	N9K-C9336C-
FX2				
node2	/cdp			
	e0a	cs1-new	Ethernet1/1/1	N9K-C9336C-
FX2				
	e0b	cs2-new	Ethernet1/1/2	N9K-C9336C-
FX2				

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

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

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

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

```
cs1-new# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-      Type      Protocol  Member Ports
Channel
```

```
-----
-----
1      Pol(SU)    Eth       LACP      Eth1/35(P)  Eth1/36(P)
```

```
cs2-new# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-      Type      Protocol  Member Ports
Channel
```

```
-----
-----
1      Pol(SU)    Eth       LACP      Eth1/35(P)  Eth1/36(P)
```

22. Enable auto-revert on the cluster LIFs.

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

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

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

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

25. Ping the remote cluster interfaces to verify connectivity: `cluster ping-cluster -node <name>`

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

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

ONTAP 9.8 and later

Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the following two commands: `system switch ethernet log setup-password` and `system switch ethernet log enable-collection`

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

Enter: `system switch ethernet log setup-password`

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

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1-new
```

```
cs2-new
```

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

```
Enter the switch name: cs1-new
```

```
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
```

```
Do you want to continue? {y|n}::[n] y
```

```
Enter the password: <password of switch's admin user>
```

```
Enter the password again: <password of switch's admin user>
```

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

```
Enter the switch name: cs2-new
```

```
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
```

```
Do you want to continue? {y|n}:: [n] y
```

```
Enter the password: <password of switch's admin user>
```

```
Enter the password again: <password of switch's admin user>
```

Followed by: `system switch ethernet log enable-collection`

```
cluster1::*> system switch ethernet log enable-collection
```

Do you want to enable cluster log collection for all nodes in the cluster?

```
{y|n}: [n] y
```

Enabling cluster switch log collection.

```
cluster1::*>
```

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

ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases

Enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: `system cluster-switch log setup-password` and `system cluster-switch log enable-collection`

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

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

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

Enter the switch name: <return>

The switch name entered is not recognized.

Choose from the following list:

cs1-new

cs2-new

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

Enter the switch name: **cs1-new**

RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc

Do you want to continue? {y|n}::[n] **y**

Enter the password: <password of switch's admin user>

Enter the password again: <password of switch's admin user>

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

Enter the switch name: **cs2-new**

RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1

Do you want to continue? {y|n}:: [n] **y**

Enter the password: <password of switch's admin user>

Enter the password again: <password of switch's admin user>

Followed by: `system cluster-switch log enable-collection`

```
cluster1::*> system cluster-switch log enable-collection
```

```
Do you want to enable cluster log collection for all nodes in the  
cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```

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

27. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=END`

Migrate to a two-node switched cluster with Cisco Nexus 9336C-FX2 cluster switches

Migrate to a two-node switched cluster with Cisco Nexus 9336C-FX2 cluster switches

You must be aware of certain configuration information, port connections, and cabling requirements when you migrate a two-node switchless cluster, non-disruptively, to a cluster with Cisco Nexus 9336C-FX2 cluster switches. The procedure you use depends on whether you have two dedicated cluster-network ports on each controller or a single cluster port on each controller. The process documented works for all nodes using optical or Twinax ports but is not supported on this switch if nodes are using onboard 10Gb BASE-T RJ45 ports for the cluster-network ports.

Most systems require two dedicated cluster-network ports on each controller. See [Cisco Ethernet switches](#)

How to migrate to a switched NetApp cluster environment with Cisco Nexus 9336C-FX2 cluster switches

If you have an existing two-node switchless cluster environment, you can migrate to a two-node switched cluster environment using Cisco Nexus 9336C-FX2 switches to enable you to scale beyond two nodes in the cluster.

Two-node switchless configuration:

- The two-node switchless configuration must be properly set up and functioning.
- The nodes must be running ONTAP 9.8 and later.
- All cluster ports must be in the up state.

- All cluster logical interfaces (LIFs) must be in the up state and on their home ports.

Cisco Nexus 9336C-FX2 switch configuration:

- Both switches must have management network connectivity.
- There must be console access to the cluster switches.
- Nexus 9336C-FX2 node-to-node switch and switch-to-switch connections must use Twinax or fiber cables.

The [Hardware Universe - Switches](#) contains more information about cabling.

[Hardware Universe - Switches](#)

- Inter-Switch Link (ISL) cables must be connected to ports 1/35 and 1/36 on both 9336C-FX2 switches.
- Initial customization of both the 9336C-FX2 switches must be completed. So that the:
 - 9336C-FX2 switches are running the latest version of software
 - Reference Configuration Files (RCFs) have been applied to the switches Any site customization, such as SMTP, SNMP, and SSH must be configured on the new switches.

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

- The names of the 9336C-FX2 switches are cs1 and cs2.
- The names of the cluster SVMs are node1 and node2.
- The names of the LIFs are node1_clus1 and node1_clus2 on node 1, and node2_clus1 and node2_clus2 on node 2 respectively.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The cluster ports used in this procedure are e0a and e0b.

The [Hardware Universe](#) contains the latest information about the actual cluster ports for your platforms.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=xh`

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



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

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

The advanced prompt (`*>`) appears.

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

You must not disable the ISL ports.

The following example shows that node-facing ports 1 through 34 are disabled on switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e/1-34
cs1(config-if-range)# shutdown
```

4. Verify that the ISL and the physical ports on the ISL between the two 9336C-FX2 switches cs1 and cs2 are up on ports 1/35 and 1/36: `show port-channel summary`

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

```
cs1# show port-channel summary

Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
      Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/35 (P)  Eth1/36 (P)
```

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

```
(cs2)# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/35 (P)  Eth1/36 (P)
```

5. Display the list of neighboring devices: `show cdp neighbors`

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

The following example lists the neighboring devices on switch cs1:

```
cs1# show cdp neighbors
```

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

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port
cs2	Eth1/35	175	R S I s	N9K-C9336C	
Eth1/35					
cs2	Eth1/36	175	R S I s	N9K-C9336C	
Eth1/36					

```
Total entries displayed: 2
```

The following example lists the neighboring devices on switch cs2:

```
cs2# show cdp neighbors
```

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

Device-ID ID	Local Intrfce	Hldtme	Capability	Platform	Port
cs1 Eth1/35	Eth1/35	177	R S I s	N9K-C9336C	
cs1 Eth1/36	Eth1/36	177	R S I s	N9K-C9336C	

Total entries displayed: 2

6. Verify that all cluster ports are up: `network port show -ipSpace Cluster`

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

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

Node: node1

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

Node: node2

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

4 entries were displayed.

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

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

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

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
Cluster					
true	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true	node2_clus2	up/up	169.254.19.183/16	node2	e0b

4 entries were displayed.

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

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

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

4 entries were displayed.

9. Disconnect the cable from cluster port e0a on node1, and then connect e0a to port 1 on cluster switch cs1, using the appropriate cabling supported by the 9336C-FX2 switches.

The [Hardware Universe - Switches](#) contains more information about cabling.

[Hardware Universe - Switches](#)

10. Disconnect the cable from cluster port e0a on node2, and then connect e0a to port 2 on cluster switch cs1, using the appropriate cabling supported by the 9336C-FX2 switches.
11. Enable all node-facing ports on cluster switch cs1.

The following example shows that ports 1/1 through 1/34 are enabled on switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-34
cs1(config-if-range)# no shutdown
```

12. Verify that all cluster LIFs are up, operational, and display as true for Is Home:network interface show -vserver Cluster

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

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

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

Cluster					
true	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

4 entries were displayed.

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

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

```
cluster1::*> cluster show
```

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

```
2 entries were displayed.
```

14. Disconnect the cable from cluster port e0b on node1, and then connect e0b to port 1 on cluster switch cs2, using the appropriate cabling supported by the 9336C-FX2 switches.
15. Disconnect the cable from cluster port e0b on node2, and then connect e0b to port 2 on cluster switch cs2, using the appropriate cabling supported by the 9336C-FX2 switches.
16. Enable all node-facing ports on cluster switch cs2.

The following example shows that ports 1/1 through 1/34 are enabled on switch cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-34
cs2(config-if-range)# no shutdown
```

17. Verify that all cluster ports are up: `network port show -ip space Cluster`

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

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

Node: node1

Ignore

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

Node: node2

Ignore

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

4 entries were displayed.

18. Verify that all interfaces display true for `Is Home: network interface show -vserver Cluster`



This might take several minutes to complete.

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

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

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

Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

```
4 entries were displayed.
```

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

The following example shows the appropriate results for both switches:

```
(cs1)# show cdp neighbors
```

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

Device-ID ID	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	133	H	FAS2980	e0a
node2	Eth1/2	133	H	FAS2980	e0a
cs2	Eth1/35	175	R S I s	N9K-C9336C	
Eth1/35					
cs2	Eth1/36	175	R S I s	N9K-C9336C	
Eth1/36					

Total entries displayed: 4

```
(cs2)# show cdp neighbors
```

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

Device-ID ID	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	133	H	FAS2980	e0b
node2	Eth1/2	133	H	FAS2980	e0b
cs1	Eth1/35	175	R S I s	N9K-C9336C	
Eth1/35					
cs1	Eth1/36	175	R S I s	N9K-C9336C	
Eth1/36					

Total entries displayed: 4

20. Display information about the discovered network devices in your cluster: network device-discovery
show -protocol cdp

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	0/2	N9K-
C9336C				
	e0b	cs2	0/2	N9K-
C9336C				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C9336C				
	e0b	cs2	0/1	N9K-
C9336C				

4 entries were displayed.

21. Verify that the settings are disabled: `network options switchless-cluster show`



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

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

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

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

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

```
cluster1::*> cluster show
```

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

23. Ensure that the cluster network has full connectivity: `cluster ping-cluster -node node-name`

```

cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

24. Change the privilege level back to admin: `set -privilege admin`
25. For ONTAP 9.8 and later, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: `system switch ethernet log setup-password` and `system switch ethernet log enable-collection`

```

cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>

```



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

26. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: `system cluster-switch log setup-password` and `system cluster-switch log enable-collection`


```

cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>

```



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

27. If you suppressed automatic case creation, reenable it by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=END`

Configure a Cisco Nexus 9336C-FX2 cluster switch

Configure a Cisco Nexus 9336C-FX2 cluster switch

You can configure a new Nexus 9336C-FX2 switch by completing the steps detailed in

this chapter.

Installing the Nexus 9336C-FX2 switch on systems running ONTAP 9.8 and later, starts with setting up an IP address and configuration to allow the switch to communicate through the management interface. You can then install the NX-OS software and reference configuration file (RCF). This procedure is intended for preparing the Nexus 9336C-FX2 switch before controllers are added.

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

- The Nexus 9336C-FX2 switch names are cs1 and cs2.
- The example used in this procedure starts the upgrade on the second switch, *cs2*.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The IPspace name is Cluster.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The cluster ports on each node are named e0a and e0b.

See the [Hardware Universe](#) for the actual cluster ports supported on your platform.

- The node connections supported for the Nexus 9336C-FX2 switches are ports 1/1 through 1/34.
- The Inter-Switch Links (ISLs) supported for the Nexus 9336C-FX2 switches are ports 1/35 and 1/36.
- The examples in this procedure use two nodes, but you can have up to 24 nodes in a cluster.

Initial installation of the Nexus 9336C-FX2 cluster switch

You can use this procedure to perform the initial installation of the Cisco Nexus 9336C-FX2 switch.

You can download the applicable NetApp Cisco NX-OS software for your switches from the NetApp Support Site at mysupport.netapp.com.

NX-OS is a network operating system for the Nexus series of Ethernet switches and MDS series of Fibre Channel (FC) storage area network switches provided by Cisco Systems.

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

Steps

1. Connect the serial port to the host or serial port of your choice.
2. Connect the management port (on the non-port side of the switch) to the same network where your SFTP server is located.
3. At the console, set the host side serial settings:
 - 9600 baud
 - 8 data bits
 - 1 stop bit
 - parity: none
 - flow control: none
4. Booting for the first time or rebooting after erasing the running configuration, the Nexus 9336C-FX2 switch

loops in a boot cycle. Interrupt this cycle by typing **yes** to abort Power on Auto Provisioning. You are then presented with the System Admin Account setup:

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

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

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

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

6. Enter and confirm the password for user admin:

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

7. Enter the Basic System Configuration dialog:

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

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

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

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

8. Create another login account:

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

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

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

10. Configure the cluster switch name:

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

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

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)  
[y]: y  
  
Mgmt0 IPv4 address : 172.22.133.216  
  
Mgmt0 IPv4 netmask : 255.255.224.0  
  
Configure the default gateway? (yes/no) [y]: y  
  
IPv4 address of the default gateway : 172.22.128.1
```

12. Configure advanced IP options:

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

13. Configure Telnet services:

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

14. Configure SSH services and SSH keys:

```
Enable the ssh service? (yes/no) [y]: y  
  
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa  
  
Number of rsa key bits <1024-2048> [1024]: 2048
```

15. Configure other settings:

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

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

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

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

16. Confirm switch information and save the configuration:

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

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

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

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

```

cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>

```



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

18. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: `system cluster-switch log setup-password` and `system cluster-switch log enable-collection`

```

cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>

```



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

Install the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 9336C-FX2 cluster switch.

Steps

1. Connect the cluster switch to the management network.

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

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

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

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

3. Copy the NX-OS software and EPLD images to the Nexus 9336C-FX2 switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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


```
cs2# show version
```

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

```
TAC support: http://www.cisco.com/tac
```

```
Copyright (C) 2002-2020, Cisco and/or its affiliates.
```

```
All rights reserved.
```

```
The copyrights to certain works contained in this software are  
owned by other third parties and used and distributed under their own  
licenses, such as open source. This software is provided "as is," and  
unless
```

```
otherwise stated, there is no warranty, express or implied, including  
but not
```

```
limited to warranties of merchantability and fitness for a particular  
purpose.
```

```
Certain components of this software are licensed under  
the GNU General Public License (GPL) version 2.0 or  
GNU General Public License (GPL) version 3.0 or the GNU  
Lesser General Public License (LGPL) Version 2.1 or  
Lesser General Public License (LGPL) Version 2.0.
```

```
A copy of each such license is available at
```

```
http://www.opensource.org/licenses/gpl-2.0.php and
```

```
http://opensource.org/licenses/gpl-3.0.html and
```

```
http://www.opensource.org/licenses/lgpl-2.1.php and
```

```
http://www.gnu.org/licenses/old-licenses/library.txt.
```

Software

```
BIOS: version 08.38
```

```
NXOS: version 9.3(4)
```

```
BIOS compile time: 05/29/2020
```

```
NXOS image file is: bootflash:///nxos.9.3.4.bin
```

```
NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]
```

Hardware

```
cisco Nexus9000 C9336C-FX2 Chassis
```

```
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
```

```
Processor Board ID FOC20291J6K
```

```
Device name: cs2
```

```
bootflash: 53298520 kB
```

```
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov 2 18:32:06 2020
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

5. Install the NX-OS image.

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

```
cs2# install all nxos bootflash:nxos.9.3.5.bin

Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
[#####] 100% -- SUCCESS

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

Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
[#####] 100% -- SUCCESS

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

Notifying services about system upgrade.
[#####] 100% -- SUCCESS


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

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-Version
Upg-Required			
1	nxos	9.3(4)	9.3(5)
yes			
1	bios	v08.37(01/28/2020):v08.23(09/23/2015)	
v08.38(05/29/2020)		yes	

Switch will be reloaded for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

Performing runtime checks.

[#####] 100% -- SUCCESS

Setting boot variables.

[#####] 100% -- SUCCESS

Performing configuration copy.

[#####] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.

Warning: please do not remove or power off the module at this time.

[#####] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.

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

```
cs2# show version
```

Cisco Nexus Operating System (NX-OS) Software

TAC support: <http://www.cisco.com/tac>

Copyright (C) 2002-2020, Cisco and/or its affiliates.

All rights reserved.

The copyrights to certain works contained in this software are owned by other third parties and used and distributed under their own licenses, such as open source. This software is provided "as is," and unless

otherwise stated, there is no warranty, express or implied, including

but not
limited to warranties of merchantability and fitness for a particular
purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
<http://www.opensource.org/licenses/gpl-2.0.php> and
<http://opensource.org/licenses/gpl-3.0.html> and
<http://www.opensource.org/licenses/lgpl-2.1.php> and
<http://www.gnu.org/licenses/old-licenses/library.txt>.

Software

BIOS: version 05.33
NXOS: version 9.3(5)
BIOS compile time: 09/08/2018
NXOS image file is: bootflash:///nxos.9.3.5.bin
NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]

Hardware

cisco Nexus9000 C9336C-FX2 Chassis
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.
Processor Board ID FOC20291J6K

Device name: cs2
bootflash: 53298520 kB

Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)

Last reset at 277524 usecs after Mon Nov 2 22:45:12 2020

Reason: Reset due to upgrade

System version: 9.3(4)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

7. Upgrade the EPLD image and reboot the switch.

```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

8. After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

```
cs2# show version module 1 epld
```

EPLD Device		Version

MI	FPGA	0x7
IO	FPGA	0x19
MI	FPGA2	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2

Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 9336C-FX2 switch for the first time. You can also use this procedure to upgrade your RCF version.

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

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



- The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated.
- Before performing this procedure, make sure that you have a current backup of the switch configuration.

Steps

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

```

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

```

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

- a. Verify that all the cluster ports are up with a healthy status: `network port show -role cluster`

```

cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore

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

```

Node: cluster1-02

Ignore

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

8 entries were displayed.

Node: cluster1-03

Ignore

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

Node: cluster1-04

Ignore

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

cluster1::*>

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

cluster

```
cluster1::*> network interface show -role cluster
```

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

Cluster					
01	e0a	cluster1-01_clus1 true	up/up	169.254.3.4/23	cluster1-
01	e0d	cluster1-01_clus2 true	up/up	169.254.3.5/23	cluster1-
02	e0a	cluster1-02_clus1 true	up/up	169.254.3.8/23	cluster1-
02	e0d	cluster1-02_clus2 true	up/up	169.254.3.9/23	cluster1-
03	e0a	cluster1-03_clus1 true	up/up	169.254.1.3/23	cluster1-
03	e0b	cluster1-03_clus2 true	up/up	169.254.1.1/23	cluster1-
04	e0a	cluster1-04_clus1 true	up/up	169.254.1.6/23	cluster1-
04	e0b	cluster1-04_clus2 true	up/up	169.254.1.7/23	cluster1-

8 entries were displayed.
cluster1::*>

- c. Verify that the cluster displays information for both cluster switches: `system cluster-switch show -is-monitoring-enabled-operational true`

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
```

Switch	Type	Address	Model
cs1	cluster-network	10.233.205.90	N9K-C9336C
Serial Number: FOCXXXXXXGD Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5) Version Source: CDP			
cs2	cluster-network	10.233.205.91	N9K-C9336C
Serial Number: FOCXXXXXXGS Is Monitored: true Reason: None Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 9.3(5) Version Source: CDP			

```
cluster1::*>
```

3. Disable auto-revert on the cluster LIFs.

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

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

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

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

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

```

cluster1::*> network interface show -role cluster

```

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

Cluster				
e0a	true	cluster1-01_clus1 up/up	169.254.3.4/23	cluster1-01
e0a	false	cluster1-01_clus2 up/up	169.254.3.5/23	cluster1-01
e0a	true	cluster1-02_clus1 up/up	169.254.3.8/23	cluster1-02
e0a	false	cluster1-02_clus2 up/up	169.254.3.9/23	cluster1-02
e0a	true	cluster1-03_clus1 up/up	169.254.1.3/23	cluster1-03
e0a	false	cluster1-03_clus2 up/up	169.254.1.1/23	cluster1-03
e0a	true	cluster1-04_clus1 up/up	169.254.1.6/23	cluster1-04
e0a	false	cluster1-04_clus2 up/up	169.254.1.7/23	cluster1-04

```

8 entries were displayed.
cluster1::*>

```

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

```

cluster1::*> cluster show

```

Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

```

4 entries were displayed.
cluster1::*>

```

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

```
show running-config
```

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

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

- b. Perform a basic setup of the switch.
9. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 9000 Series NX-OS Command Reference](#) guides.

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

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

10. Apply the RCF previously downloaded to the bootflash.

For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 9000 Series NX-OS Command Reference](#) guides.

This example shows the RCF file `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` being installed on switch cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
```

11. Examine the banner output from the `show banner motd` command. You must read and follow these instructions to ensure the proper configuration and operation of the switch.

```
cs2# show banner motd
```

```
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Nexus N9K-C9336C-FX2
* Filename  : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date      : 10-23-2020
* Version   : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int e1/1/1-4,
e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int e1/4/1-
4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G configuration
in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

12. Verify that the RCF file is the correct newer version: `show running-config`

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

- The RCF banner

- The node and port settings
- Customizations The output varies according to your site configuration. Check the port settings and refer to the release notes for any changes specific to the RCF that you have installed.

13. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file.

For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 9000 Series NX-OS Command Reference](#) guides.

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

14. Reboot switch cs2. You can ignore the “cluster ports down” events reported on the nodes while the switch reboots.

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

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

- Verify that e0d ports are up and healthy across all nodes in the cluster: `network port show -role cluster`

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

Node: cluster1-01

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

Node: cluster1-02

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

```

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

Node: cluster1-03

Ignore

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

Node: cluster1-04

Ignore

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

```

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

```

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

```

```

cluster1-01/cdp
    e0a    cs1                                Ethernet1/7    N9K-
C9336C
    e0d    cs2                                Ethernet1/7    N9K-
C9336C
cluster01-2/cdp
    e0a    cs1                                Ethernet1/8    N9K-
C9336C
    e0d    cs2                                Ethernet1/8    N9K-
C9336C
cluster01-3/cdp
    e0a    cs1                                Ethernet1/1/1  N9K-
C9336C
    e0b    cs2                                Ethernet1/1/1  N9K-
C9336C
cluster1-04/cdp
    e0a    cs1                                Ethernet1/1/2  N9K-
C9336C
    e0b    cs2                                Ethernet1/1/2  N9K-
C9336C

```

```

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true

```

Switch	Type	Address	Model
cs1	cluster-network	10.233.205.90	NX9-

```

C9336C
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

```

```

cs2                                cluster-network    10.233.205.91    NX9-
C9336C
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

```

```

2 entries were displayed.

```




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

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER: Blocking
port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL: Blocking
port-channel1 on VLAN0092. Inconsistent local vlan.
```

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

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

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

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

```

cluster1::*> network interface show -role cluster

```

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	false			
	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	true			
	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	false			
	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0d	true			
	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0b	false			
	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0b	true			
	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0b	false			
	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04
e0b	true			

```

8 entries were displayed.
cluster1::*>

```

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

```

cluster1::*> cluster show

```

Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

```

4 entries were displayed.
cluster1::*>

```

19. Repeat Steps 7 to 14 on switch cs1.

20. Enable auto-revert on the cluster LIFs.

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

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

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

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

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

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

```
cs1# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lACP mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-      Type      Protocol  Member Ports      Channel
-----
-----
1      Po1 (SU)    Eth       LACP             Eth1/35 (P)        Eth1/36 (P)
cs1#
```

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

```

cluster1::*> network interface show -role cluster

```

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

Cluster				
e0d	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0b	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0b	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0b	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0b	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04

```

8 entries were displayed.
cluster1::*>

```

25. Verify that the cluster is healthy: cluster show

```

cluster1::*> cluster show

```

Node	Health	Eligibility	Epsilon
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

```

4 entries were displayed.
cluster1::*>

```

26. Ping the remote cluster interfaces to verify connectivity: cluster ping-cluster -node local

```

cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)

```

Replace a Cisco Nexus 9336C-FX2 cluster switch

Replacing a defective Nexus 9336C-FX2 switch in a cluster network is a nondisruptive procedure (NDU).

Before you begin

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

- Existing cluster and network infrastructure:
 - The existing cluster must be verified as completely functional, with at least one fully connected cluster switch.
 - All cluster ports must be up.
 - All cluster logical interfaces (LIFs) must be up and on their home ports.
 - The ONTAP cluster ping-cluster -node node1 command must indicate that basic connectivity and larger than PMTU communication are successful on all paths.
- Nexus 9336C-FX2 replacement switch:
 - Management network connectivity on the replacement switch must be functional.
 - Console access to the replacement switch must be in place.
 - The node connections are ports 1/1 through 1/34.
 - All Inter-Switch Link (ISL) ports must be disabled on ports 1/35 and 1/36.
 - The desired reference configuration file (RCF) and NX-OS operating system image switch must be loaded onto the switch.
 - Initial customization of the switch must be complete, as detailed in:

[Configuring a new Cisco Nexus 9336C-FX2 switch](#)

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

You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.

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

- The names of the existing Nexus 9336C-FX2 switches are cs1 and cs2.
- The name of the new Nexus 9336C-FX2 switch is newcs2.
- The node names are node1 and node2.
- The cluster ports on each node are named e0a and e0b.
- The cluster LIF names are node1_clus1 and node1_clus2 for node1, and node2_clus1 and node2_clus2 for node2.
- The prompt for changes to all cluster nodes is cluster1::*>



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

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

```
Node: node1
```

```
Ignore
```

```
Speed (Mbps) Health
```

```
Health
```

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
-----	-----	-----	-----	----	----	-----	-----

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

Node: node2

Ignore

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

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

4 entries were displayed.

cluster1::*> network interface show -vserver Cluster

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

Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

4 entries were displayed.


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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	Eth1/2	N9K-C9336C
	e0b	cs2	Eth1/2	N9K-C9336C
node1	/cdp			
	e0a	cs1	Eth1/1	N9K-C9336C
	e0b	cs2	Eth1/1	N9K-C9336C

4 entries were displayed.

```
cs1# show cdp neighbors
```

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

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
node1	Eth1/1	144	H	FAS2980	e0a
node2	Eth1/2	145	H	FAS2980	e0a
cs2	Eth1/35	176	R S I s	N9K-C9336C	Eth1/35
cs2 (FDO220329V5)	Eth1/36	176	R S I s	N9K-C9336C	Eth1/36

Total entries displayed: 4

```
cs2# show cdp neighbors
```

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

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port ID
node1	Eth1/1	139	H	FAS2980	e0b
node2	Eth1/2	124	H	FAS2980	e0b
cs1	Eth1/35	178	R S I s	N9K-C9336C	Eth1/35
cs1	Eth1/36	178	R S I s	N9K-C9336C	Eth1/36

Total entries displayed: 4

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=xh`

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



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

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

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

- a. Go to the *NetApp Cluster and Management Network Switches Reference Configuration File Description Page* on the NetApp Support Site.
 - b. Click the link for the *Cluster Network and Management Network Compatibility Matrix*, and then note the required switch software version.
 - c. Click your browser's back arrow to return to the Description page, click **CONTINUE**, accept the license agreement, and then go to the Download page.
 - d. Follow the steps on the Download page to download the correct RCF and NX-OS files for the version of ONTAP software you are installing.
3. On the new switch, log in as admin and shut down all of the ports that will be connected to the node cluster interfaces (ports 1/1 to 1/34).

If the switch that you are replacing is not functional and is powered down, go to Step 4. The LIFs on the cluster nodes should have already failed over to the other cluster port for each node.

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-34
newcs2(config-if-range)# shutdown
```

4. Verify that all cluster LIFs have auto-revert enabled: `network interface show -vserver Cluster -fields auto-revert`

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

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

4 entries were displayed.

5. Verify that all the cluster LIFs can communicate: `cluster ping-cluster`

```
cluster1::*> cluster ping-cluster node1
```

Host is node2

Getting addresses from network interface table...

Cluster node1_clus1 169.254.209.69 node1 e0a

Cluster node1_clus2 169.254.49.125 node1 e0b

Cluster node2_clus1 169.254.47.194 node2 e0a

Cluster node2_clus2 169.254.19.183 node2 e0b

Local = 169.254.47.194 169.254.19.183

Remote = 169.254.209.69 169.254.49.125

Cluster Vserver Id = 4294967293

Ping status:

....

Basic connectivity succeeds on 4 path(s)

Basic connectivity fails on 0 path(s)

.....

Detected 9000 byte MTU on 4 path(s):

Local 169.254.47.194 to Remote 169.254.209.69

Local 169.254.47.194 to Remote 169.254.49.125

Local 169.254.19.183 to Remote 169.254.209.69

Local 169.254.19.183 to Remote 169.254.49.125

Larger than PMTU communication succeeds on 4 path(s)

RPC status:

2 paths up, 0 paths down (tcp check)

2 paths up, 0 paths down (udp check)

6. Shut down the ISL ports 1/35 and 1/36 on the Nexus 9336C-FX2 switch cs1:

```

cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/35-36
cs1(config-if-range)# shutdown
cs1(config-if-range)#

```

7. Remove all of the cables from the Nexus 9336C-FX2 cs2 switch, and then connect them to the same ports on the Nexus C9336C-FX2 newcs2 switch.
8. Bring up the ISLs ports 1/35 and 1/36 between the cs1 and newcs2 switches, and then verify the port channel operation status.

Port-Channel should indicate Po1(SU) and Member Ports should indicate Eth1/35(P) and Eth1/36(P).

This example enables ISL ports 1/35 and 1/36 and displays the port channel summary on switch cs1:

```

cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/35-36
cs1(config-if-range)# no shutdown

cs1(config-if-range)# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member      Ports
      Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/35 (P)  Eth1/36 (P)

cs1(config-if-range)#

```

9. Verify that port e0b is up on all nodes: `network port show ipspace Cluster`

The output should be similar to the following:

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

```
Node: node1
```

```
Ignore
```

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

```
Node: node2
```

```
Ignore
```

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

```
4 entries were displayed.
```

10. On the same node you used in the previous step, revert the cluster LIF associated with the port in the previous step by using the network interface revert command.

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

The following commands return LIF node1_clus2 on node1 to home port e0a and displays information about the LIFs on both nodes. Bringing up the first node is successful if the Is Home column is true for both cluster interfaces and they show the correct port assignments, in this example e0a and e0b on node1.

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

Current Is Vserver Home	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Port
Cluster	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true	node2_clus2	up/up	169.254.19.183/16	node2	e0a
false					

4 entries were displayed.

11. Display information about the nodes in a cluster: `cluster show`

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

```
cluster1::*> cluster show
```

Node	Health	Eligibility
node1	false	true
node2	true	true

12. Verify that all physical cluster ports are up: `network port show ipspace Cluster`

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

```
Node node1
```

```
Ignore
```

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

```
4 entries were displayed.
```

13. Verify that all the cluster LIFs can communicate: `cluster ping-cluster`

```

cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

14. Confirm the following cluster network configuration: network port show

```

cluster1::*> network port show -ipspace Cluster
Node: node1

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

Node: node2

```


Ignore

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

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

4 entries were displayed.

cluster1::*> network interface show -vserver Cluster

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

Cluster						
	node1_clus1	up/up	169.254.209.69/16	node1	e0a	
true						
	node1_clus2	up/up	169.254.49.125/16	node1	e0b	
true						
	node2_clus1	up/up	169.254.47.194/16	node2	e0a	
true						
	node2_clus2	up/up	169.254.19.183/16	node2	e0b	
true						

4 entries were displayed.

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

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

node2	/cdp				
	e0a	cs1	0/2		N9K-
C9336C					
	e0b	newcs2	0/2		N9K-
C9336C					

```

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

```

4 entries were displayed.

```
cs1# show cdp neighbors
```

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

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform	
node1	Eth1/1	144	H	FAS2980	e0a
node2	Eth1/2	145	H	FAS2980	e0a
newcs2 Eth1/35	Eth1/35	176	R S I s	N9K-C9336C	
newcs2 Eth1/36	Eth1/36	176	R S I s	N9K-C9336C	

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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	139	H	FAS2980	e0b
node2	Eth1/2	124	H	FAS2980	e0b
cs1 Eth1/35	Eth1/35	178	R S I s	N9K-C9336C	
cs1 Eth1/36	Eth1/36	178	R S I s	N9K-C9336C	

Total entries displayed: 4

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

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



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

16. For ONTAP releases 9.5P16, 9.6P12, and 9.7P10 and later patch releases, enable the Ethernet switch health monitor log collection feature for collecting switch-related log files, using the commands: `system cluster-switch log setup-password` and `system cluster-switch log enable-collection`

```

cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

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

Enter the switch name: cs1
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>

```



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

17. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=END`

Replace a Cisco Nexus 9336C-FX2 storage switch

You must be aware of certain configuration information, port connections and cabling requirements when you replace Cisco Nexus 9336C-FX2 storage switches.

Before you begin

You must verify that the following conditions exist before installing the NX-OS software and RCFs on a Cisco Nexus 9336C-FX2 storage switch:

- Your system can support Cisco Nexus 9336C-FX2 storage switches.
- You must have consulted the switch compatibility table on the Cisco Ethernet Switch page for the supported ONTAP, NX-OS, and RCF versions.



You should be aware that there can be dependencies between command syntax in the RCF and NX-OS versions.

- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures. Cisco Nexus 3000 Series Switches
- You must have downloaded the applicable RCFs.

About this task

The existing network configuration must have the following characteristics:

- The Cisco Ethernet Switches page has the latest RCF and NX-OS versions on your switches.
- Management connectivity must exist on both switches.



Make sure that all troubleshooting steps have been completed to confirm that your switch needs replacing.

The replacement Cisco Nexus 9336C-FX2 switch must have the following characteristics:

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

Procedure summary

This procedure replaces the second Nexus 9336C-FX2 storage switch S2 with the new 9336C-FX2 switch NS2. The two nodes are node1 and node2.

Steps to complete:

- Confirm the switch to be replaced is S2.
- Disconnect the cables from switch S2.
- Reconnect the cables to switch NS2.
- Verify all device configurations on switch NS2.

Steps

1. If AutoSupport is enabled on this cluster, suppress automatic case creation by invoking an AutoSupport message: `system node autosupport invoke -node * -type all - message MAINT=xh`

x is the duration of the maintenance window in hours.

2. Check on the health status of the storage node ports to make sure that there is connection to storage switch S1:

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

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

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

```
storage::*>
```

3. Verify that storage switch S1 is available: network device-discovery show

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node1/cdp				
	e3a	S1	Ethernet1/1	NX9336C
	e4a	node2	e4a	AFF-A700
	e4e	node2	e4e	AFF-A700
node1/lldp				
	e3a	S1	Ethernet1/1	-
	e4a	node2	e4a	-
	e4e	node2	e4e	-
node2/cdp				
	e3a	S1	Ethernet1/2	NX9336C
	e4a	node1	e4a	AFF-A700
	e4e	node1	e4e	AFF-A700
node2/lldp				
	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-

```
storage::*>
```

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

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf   Hold-time   Capability   Port ID
node1               Eth1/1      121         S            e3a
node2               Eth1/2      121         S            e3a
SHFGD2008000011    Eth1/5      121         S            e0a
SHFGD2008000011    Eth1/6      120         S            e0a
SHFGD2008000022    Eth1/7      120         S            e0a
SHFGD2008000022    Eth1/8      120         S            e0a
```

5. Verify the shelf ports in the storage system: `storage shelf port show -fields remote-device,remote-port`

```
storage::*> storage shelf port show -fields remote-device,remote-port
shelf  id  remote-port  remote-device
----- --  -
3.20   0  Ethernet1/5  S1
3.20   1  -            -
3.20   2  Ethernet1/6  S1
3.20   3  -            -
3.30   0  Ethernet1/7  S1
3.20   1  -            -
3.30   2  Ethernet1/8  S1
3.20   3  -            -
storage::*>
```

6. Remove all cables attached to storage switch S2.
7. Reconnect all cables to the replacement switch NS2.
8. Recheck the health status of the storage node ports: `storage port show -port-type ENET`

```

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

```

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

node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

```

storage::*>

```

9. Verify that both switches are available: network device-discovery show

```

storage::*> network device-discovery show

```

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

node1/cdp				
	e3a	S1	Ethernet1/1	NX9336C
	e4a	node2	e4a	AFF-A700
	e4e	node2	e4e	AFF-A700
	e7b	NS2	Ethernet1/1	NX9336C
node1/lldp				
	e3a	S1	Ethernet1/1	-
	e4a	node2	e4a	-
	e4e	node2	e4e	-
	e7b	NS2	Ethernet1/1	-
node2/cdp				
	e3a	S1	Ethernet1/2	NX9336C
	e4a	node1	e4a	AFF-A700
	e4e	node1	e4e	AFF-A700
	e7b	NS2	Ethernet1/2	NX9336C
node2/lldp				
	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-
	e7b	NS2	Ethernet1/2	-

```

storage::*>

```


10. Verify the shelf ports in the storage system: `storage shelf port show -fields remote-device,remote-port`

```
storage::*> storage shelf port show -fields remote-device,remote-port
shelf    id      remote-port    remote-device
-----  --      -
3.20     0      Ethernet1/5    S1
3.20     1      Ethernet1/5    NS2
3.20     2      Ethernet1/6    S1
3.20     3      Ethernet1/6    NS2
3.30     0      Ethernet1/7    S1
3.20     1      Ethernet1/7    NS2
3.30     2      Ethernet1/8    S1
3.20     3      Ethernet1/8    NS2
storage::*>
```

11. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message: `system node autosupport invoke -node * -type all -message MAINT=END`

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

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