



Cisco Nexus 9336C-FX2

Cluster and storage switches

NetApp
January 31, 2025

Table of Contents

- Cisco Nexus 9336C-FX2 1
 - Overview 1
 - Install hardware 4
 - Configure software 15
 - Replace a Cisco Nexus 9336C-FX2 storage switch 53

Cisco Nexus 9336C-FX2

Overview

Overview of installation and configuration for Cisco Nexus 9336C-FX2 storage switches

The Cisco Nexus 9336C-FX2 switch is part of the Cisco Nexus 9000 platform and can be installed in a NetApp system cabinet. The Nexus 9336C-FX2 is an Ethernet switch that allows you to switch data between controllers and disk shelves.

Initial configuration overview

To initially configure a Cisco Nexus 9336C-FX2 switch on systems running ONTAP, follow these steps:

1. [Complete cabling worksheet.](#)
2. [Install the switch.](#)
3. [Configure the switch.](#)
4. [Install the switch in a NetApp cabinet.](#)
5. [Prepare to install NX-OS and RCF.](#)
6. [Install the NX-OS software.](#)
7. [Install the RCF config file.](#)
8. [Enable SSH.](#)

Additional information

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

- [Configuration requirements](#)
- [Components and part numbers](#)
- [Required documentation](#)
- [Smart Call Home requirements](#)

Configuration requirements for Cisco Nexus 9336C-FX2 storage switches

For Cisco Nexus 9336C-FX2 switch installation and maintenance, be sure to review configuration and network requirements.

ONTAP support

From ONTAP 9.9.1, you can use Cisco Nexus 9336C-FX2 switches to combine storage and cluster functionality into a shared switch configuration.

If you want to build ONTAP clusters with more than two nodes, you need two supported network switches.

Configuration requirements

For configuration, you need the appropriate number and type of cables and cable connectors for your switches.

Depending on the type of switch you are initially configuring, you need to connect to the switch console port with the included console cable; you also need to provide specific network information.

Network requirements

You need the following network information for all switch configurations.

- IP subnet for management network traffic
- Host names and IP addresses for each of the storage system controllers and all applicable switches
- Most storage system controllers are managed through the e0M interface by connecting to the Ethernet service port (wrench icon). On AFF A800 and AFF A700s systems, the e0M interface uses a dedicated Ethernet port.
- Refer to the [Hardware Universe](#) for the latest information.

For more information about the initial configuration of your switch, see the following guide: [Cisco Nexus 9336C-FX2 Installation and Upgrade Guide](#).

Components and part numbers for Cisco Nexus 9336C-FX2 storage switches

For Cisco Nexus 9336C-FX2 switch installation and maintenance, be sure to review the list of components and part numbers.

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

Documentation requirements for Cisco Nexus 9336C-FX2 storage switches

For Cisco Nexus 9336C-FX2 switch installation and maintenance, be sure to review specific switch and controller documentation to set up your Cisco 9336-FX2 switches and ONTAP cluster.

Switch documentation

To set up the Cisco Nexus 9336C-FX2 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.
<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.

ONTAP systems documentation

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

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

Rail kit and cabinet documentation

To install a Cisco 9336-FX2 switch in a NetApp cabinet, see the following hardware documentation.

Name	Description
42U System Cabinet, Deep Guide	Describes the FRUs associated with the 42U system cabinet, and provides maintenance and FRU replacement instructions.
Install a Cisco 9336-FX2 switch in a NetApp Cabinet	Describes how to install a Cisco Nexus 9336C-FX2 switch in a four-post NetApp cabinet.

Smart Call Home requirements

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

Smart Call Home monitors the hardware and software components on your network. When a critical system configuration occurs, it generates an email-based notification and raises an alert to all the recipients that are configured in your destination profile. To use Smart Call Home, you must configure a cluster network switch to communicate using email with the Smart Call Home system. In addition, you can optionally set up your cluster network switch to take advantage of Cisco's embedded Smart Call Home support feature.

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

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

The [Cisco support site](#) contains information about the commands to configure Smart Call Home.

Install hardware

Complete the Cisco Nexus 9336C-FX2 cabling worksheet

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

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

Sample cabling worksheet

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

Cluster switch A		Cluster switch B	
Switch port	Node and port usage	Switch port	Node and port usage
1	4x100GbE node 1	1	4x100GbE node 1
2	4x100GbE node 2	2	4x100GbE node 2
3	4x100GbE node 3	3	4x100GbE node 3
4	4x100GbE node 4	4	4x100GbE node 4
5	4x100GbE node 5	5	4x100GbE node 5
6	4x100GbE node 6	6	4x100GbE node 6
7	4x100GbE node 7	7	4x100GbE node 7
8	4x100GbE node 8	8	4x100GbE node 8
9	4x100GbE node 9	9	4x100GbE node 9
10	4x100GbE node 10	10	4x100GbE node 10
11	4x100GbE node 11	11	4x100GbE node 11
12	4x100GbE node 12	12	4x100GbE node 12
13	4x100GbE node 13	13	4x100GbE node 13
14	4x100GbE node 14	14	4x100GbE node 14
15	4x100GbE node 15	15	4x100GbE node 15
16	4x100GbE node 16	16	4x100GbE node 16
17	4x100GbE node 17	17	4x100GbE node 17
18	4x100GbE node 18	18	4x100GbE node 18

Cluster switch A		Cluster switch B	
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	4x100GbE node 25	25	4x100GbE node 25
26	4x100GbE node 26	26	4x100GbE node 26
27	4x100GbE node 27	27	4x100GbE node 27
28	4x100GbE node 28	28	4x100GbE node 28
29	4x100GbE node 29	29	4x100GbE node 29
30	4x100GbE node 30	30	4x100GbE node 30
31	4x100GbE node 31	31	4x100GbE node 31
32	4x100GbE node 32	32	4x100GbE node 32
33	4x100GbE node 33	33	4x100GbE node 33
30	4x100GbE node 30	30	4x100GbE node 33
34	4x100GbE node 34	34	4x100GbE node 34
35	4x100GbE node 35	35	4x100GbE node 35
36	4x100GbE node 36	36	4x100GbE node 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	
20		20	
21		21	
22		22	

Cluster switch A		Cluster switch B	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	

Install the 9336C-FX2 storage switch

Follow this procedure to install the Cisco Nexus 9336C-FX2 storage switch.

What you'll need

- Access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.
- Applicable NX-OS version, downloaded from the [Cisco Software Download](#) page.
- Applicable licenses, network and configuration information, and cables.
- Completed [cabling worksheets](#).
- Applicable NetApp cluster network and management network RCFs downloaded from the NetApp Support Site at [mysupport.netapp.com](#). 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.
- Required switch documentation. See [Required documentation](#) for more information.

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 Install switch in NetApp cabinet for instructions to install the switch in a NetApp cabinet.
Equipment in a Telco rack	See the procedures provided in the switch hardware installation guides and the NetApp installation and setup instructions.

2. Cable the cluster network and management network switches to the controllers using the completed cabling worksheets.
3. Power on the cluster network and management network switches and controllers.

What's next?

Go to [Configure Cisco Nexus 9336C-FX2 storage switch](#).

Configure the 9336C-FX2 storage switch

Follow this procedure to configure the Cisco Nexus 9336C-FX2 switch.

What you'll need


- Access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.
- Applicable NX-OS version, downloaded from the [Cisco software download](#) page.
- Applicable licenses, network and configuration information, and cables.
- Completed [cabling worksheets](#).
- Applicable NetApp cluster network and management network RCFs downloaded from the NetApp Support Site at mysupport.netapp.com. 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.
- Required switch documentation. See [Required documentation](#) for more information.


Steps

1. Perform an initial configuration of the cluster network switches.

Provide applicable responses to the following initial setup questions when you first boot the switch. Your site's security policy defines the responses and services to enable.

Prompt	Response
Abort Auto Provisioning and continue with normal setup? (yes/no)	Respond with yes . The default is no.
Do you want to enforce secure password standard? (yes/no)	Respond with yes . The default is yes.

Prompt	Response
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. <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  SSH is recommended when using Ethernet Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security. </div>
Enter the type of SSH key you want to generate (dsa/rsa/rsa1).	The default is rsa .
Enter the number of key bits (1024-2048).	Enter the number of key bits from 1024 to 2048.
Configure the NTP server? (yes/no)	Respond with no . The default is no.

Prompt	Response
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. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  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. </div>

2. 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.
3. Check the version on the cluster network switches, and if necessary, download the NetApp-supported version of the software to the switches from the [Cisco software download](#) page.

What's next?

Optionally, you can [install a Cisco Nexus 9336C-FX2 switch in a NetApp cabinet](#). Otherwise, go to [Prepare to install NX-OS and RCF](#).

Install a Cisco Nexus 9336C-FX2 switch in a NetApp cabinet

Depending on your configuration, you might need to install the Cisco Nexus 9336C-FX2 switch and pass-through panel in a NetApp cabinet. Standard brackets are included with the switch.

What you'll need

- 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).

Required documentation

Review the initial preparation requirements, kit contents, and safety precautions in the [Cisco Nexus 9000 Series Hardware Installation Guide](#).

Steps

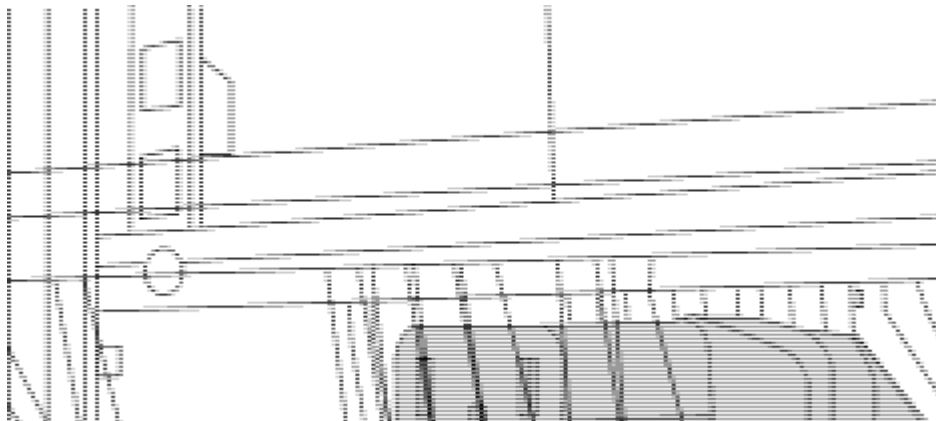
1. Install the pass-through blanking panel in the NetApp cabinet.

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

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

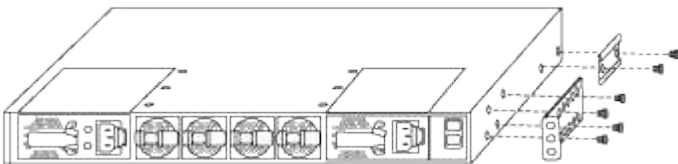
- One pass-through blanking panel
- Four 10-32 x .75 screws
- Four 10-32 clip nuts
 - a. Determine the vertical location of the switches and blanking panel in the cabinet.

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



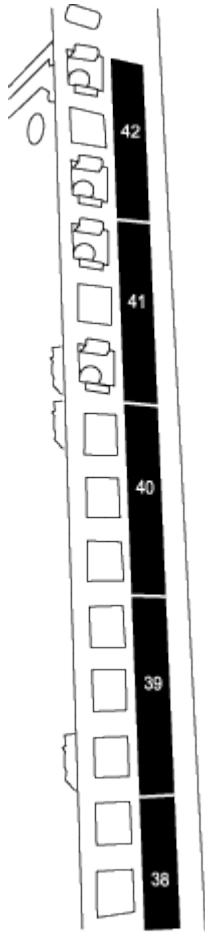
(1) Female connector of the jumper cord.

2. Install the rack-mount brackets on the Nexus 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.



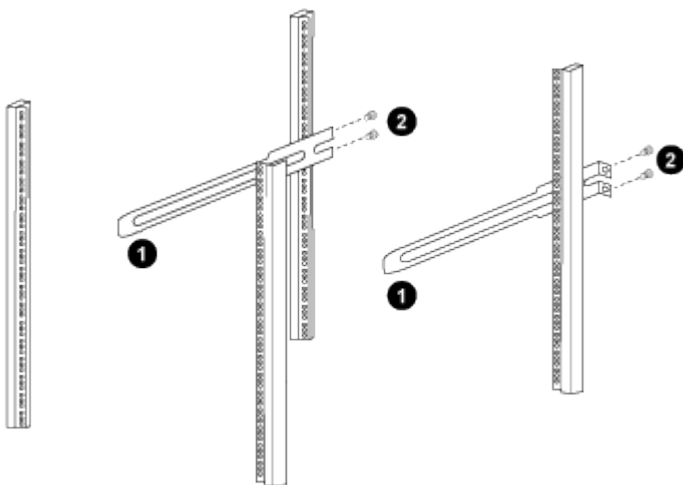
- b. Repeat step [2a](#) with the other front rack-mount bracket on the other side of the switch.
- c. Install the rear rack-mount bracket on the switch chassis.

- 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.



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

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

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

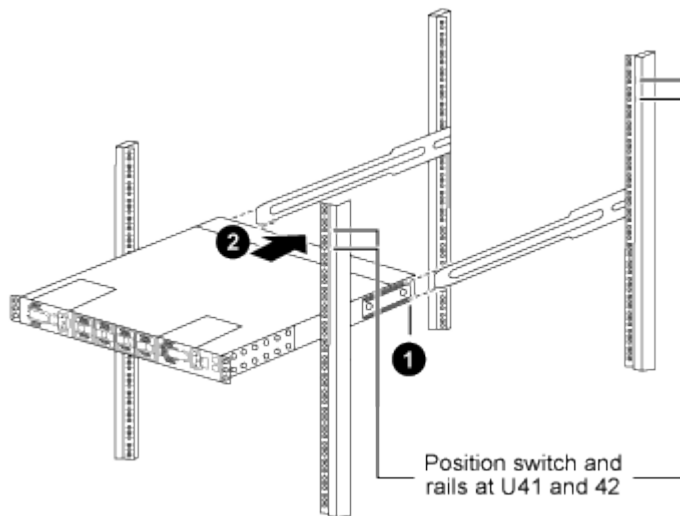
c. Repeat steps 4a and 4b at the RU41 locations on the cabinet.

5. Install the switch in the cabinet.



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

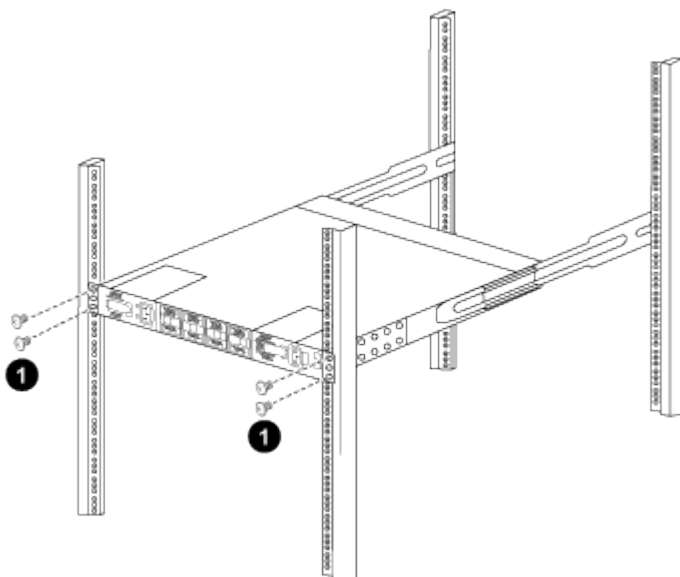
a. Position the back of the switch at RU41.



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

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

b. Attach the switch to the cabinet.



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

- c. With the chassis now supported without assistance, fully tighten the front screws to the posts.
- d. Repeat steps [5a](#) through [5c](#) for the second switch at the RU42 location.



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

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



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

8. Connect the management port on each 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.

Configure software

Software install workflow for Cisco Nexus 9336C-FX2 storage switches

To install and configure software for a Cisco Nexus 9336C-FX2 storage switch, follow these steps:

1. [Prepare to install NX-OS and RCF.](#)
2. [Install the NX-OS software.](#)
3. [Install the RCF config file.](#)

Prepare to install NX-OS software and RCF

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

About the examples

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

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

About this task

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

Steps

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

Show example

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

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

Show example

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

Node: cluster1-02

Ignore

Health Health                               Speed (Mbps)
Port     IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
-----  -----
e0a      Cluster      Cluster              up   9000  auto/100000
healthy false
e0b      Cluster      Cluster              up   9000  auto/100000
healthy false

Node: cluster1-01

Ignore

Health Health                               Speed (Mbps)
Port     IPspace      Broadcast Domain Link MTU  Admin/Oper
Status  Status
-----  -----
e0a      Cluster      Cluster              up   9000  auto/100000
healthy false
e0b      Cluster      Cluster              up   9000  auto/100000
healthy false

4 entries were displayed.
```

b. Display information about the LIFs:

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

Show example

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

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

4 entries were displayed.

5. Verify the connectivity of the remote cluster interfaces:

ONTAP 9.9.1 and later

You can use the `network interface check cluster-connectivity` command to start an accessibility check for cluster connectivity and then display the details:

```
network interface check cluster-connectivity start and network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTE: Wait for a number of seconds before running the `show` command to display the details.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	Date	LIF
Loss		
-----	-----	-----
-----	-----	-----
node1		
3/5/2024 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-
clus1 none		
3/5/2024 19:21:20 -06:00	cluster1-01_clus2	cluster1-
02_clus2 none		
node2		
3/5/2024 19:21:18 -06:00	cluster1-02_clus2	cluster1-
01_clus1 none		
3/5/2024 19:21:20 -06:00	cluster1-02_clus2	cluster1-
01_clus2 none		

All ONTAP releases

For all ONTAP releases, you can also use the `cluster ping-cluster -node <name>` command to check the connectivity:

```
cluster ping-cluster -node <name>
```

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

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

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

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

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

Show example

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

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.

What's next?

[Install the NX-OS software.](#)

Install the NX-OS software

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

Before you begin, complete the procedure in [Prepare to install NX-OS and RCF](#).

Review requirements

What you'll need

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs or similar issues).

Suggested documentation

- [Cisco Ethernet switch page](#)

Consult the switch compatibility table for the supported ONTAP and NX-OS versions.

- [Software Upgrade and downgrade guides](#)

Refer to the appropriate software and upgrade guides available on the Cisco website for complete documentation on the Cisco switch upgrade and downgrade procedures.

- [Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix](#)

Provides information on Disruptive Upgrade/Downgrade for Cisco NX-OS software on Nexus 9000 Series Switches based on your current and target releases.

On the page, select **Disruptive Upgrade** and select your current release and target release from the

dropdown list.

About the examples

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

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

Install the software

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

Steps

1. Connect the cluster switch to the management network.
2. Use the ping command to verify connectivity to the server hosting the NX-OS software and the RCF.

Show example

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

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

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

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

```
network device-discovery show
```


Show example

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
              e0a    cs1                      Ethernet1/7      N9K-
C9336C-FX2
              e0d    cs2                      Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
              e0a    cs1                      Ethernet1/8      N9K-
C9336C-FX2
              e0d    cs2                      Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/cdp
              e0a    cs1                      Ethernet1/1/1    N9K-
C9336C-FX2
              e0b    cs2                      Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
              e0a    cs1                      Ethernet1/1/2    N9K-
C9336C-FX2
              e0b    cs2                      Ethernet1/1/2    N9K-
C9336C-FX2
cluster1::*>
```

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

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

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

Show example

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

Node: cluster1-01

Ignore

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

Node: cluster1-02

Ignore

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

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

```
Node: cluster1-04
```

```
Ignore
```

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

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

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

Show example

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

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

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

Show example

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                                     Address
Model
-----
cs1                                         cluster-network                         10.233.205.90
N9K-C9336C-FX2
  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-FX2
  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::*>
```

5. Disable auto-revert on the cluster LIFs. The cluster LIFs fail over to the partner cluster switch and remain there as you perform the upgrade procedure on the targeted switch:

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

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

Show example

```
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.
```

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

```
show version
```

Show example

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

Software
  BIOS: version 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#
```

8. Install the NX-OS image.

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

Show example

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

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

```
show version
```

Show example

```
cs2# show version
```

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

Software

```
BIOS: version 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:
```

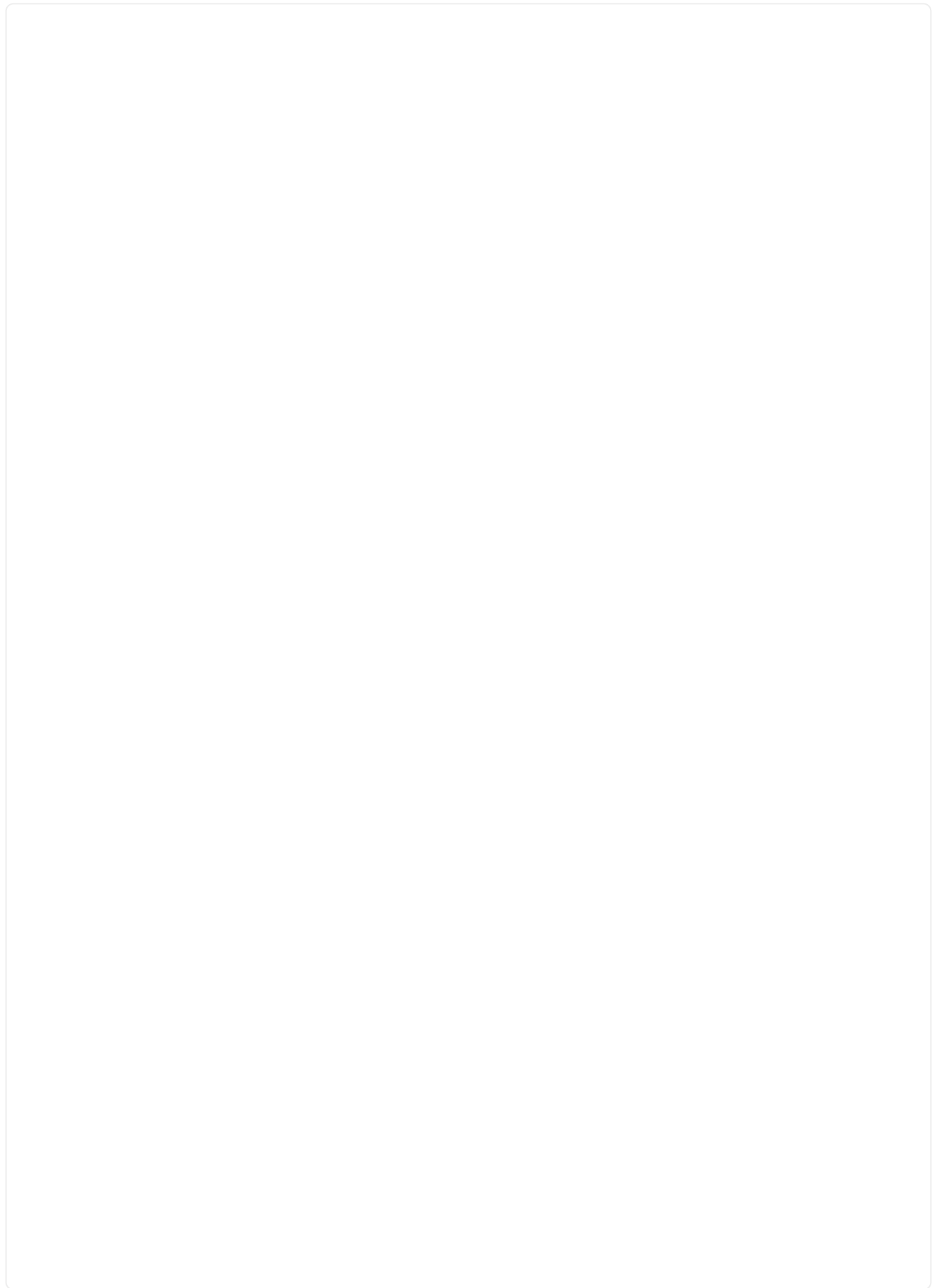
```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

10. Upgrade the EPLD image and reboot the switch.

Show example



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

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

```
cs2# install epld bootflash:n9000-epld.9.3.5.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.
```

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

Show example

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

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

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

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

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

Show example

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

```
Node: cluster1-01
```

```
Ignore
```

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

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

```
Node: cluster1-02
```

```
Ignore
```

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

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

```
Node: cluster1-03
```

```
Ignore
```

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

e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					


```
Node: cluster1-04

Ignore

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

b. Verify the switch health from the cluster.

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

Show example

```
cluster1::*> network device-discovery show -protocol cdp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                        Ethernet1/7
N9K-C9336C-FX2
          e0d    cs2                        Ethernet1/7
N9K-C9336C-FX2
cluster01-2/cdp
          e0a    cs1                        Ethernet1/8
N9K-C9336C-FX2
          e0d    cs2                        Ethernet1/8
N9K-C9336C-FX2
cluster01-3/cdp
          e0a    cs1                        Ethernet1/1/1
N9K-C9336C-FX2
          e0b    cs2                        Ethernet1/1/1
N9K-C9336C-FX2
cluster1-04/cdp
          e0a    cs1                        Ethernet1/1/2
N9K-C9336C-FX2
          e0b    cs2                        Ethernet1/1/2
N9K-C9336C-FX2

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                Type                Address
Model
-----
-----
cs1                    cluster-network    10.233.205.90
N9K-C9336C-FX2
  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-FX2
  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.

```

13. Verify that the cluster is healthy:

```
cluster show
```

Show example

```

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

```

14. Repeat steps 6 to 13 to install the NX-OS software on switch cs1.

15. Enable auto-revert on the cluster LIFs.

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

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

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

Show example

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

If any cluster LIFs have not returned to their home ports, revert them manually from the local node:

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

What's next?

[Install RCF.](#)

Install the Reference Configuration File

You install the Reference Configuration File (RCF) after setting up the Nexus 9336C-FX2 storage switch for the first time.

Before you begin

Verify the following installations and connections:

- A console connection to the switch. The console connection is optional if you have remote access to the switch.
- Switch cs1 and switch cs2 are powered up and the initial switch setup is complete (the Management IP address and SSH is set up).
- The desired NX-OS version has been installed.
- ONTAP node cluster ports are not connected.

Step 1: Install the RCF on the switches

1. Login to switch cs1 using SSH or by using a serial console.
2. Copy the RCF to the bootflash of switch cs1 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](#).

Show example

This example shows TFTP being used to copy an RCF to the bootflash on switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Storage.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)...
```

3. 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](#).

Show example

This example shows the RCF `Nexus_9336C_RCF_v1.6-Storage.txt` being installed on switch cs1:

```
cs1# copy NNexus_9336C_RCF_v1.6-Storage.txt running-config echo-
commands
```

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

Show example

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Storage.txt
* Date       : 10-23-2020
* Version    : v1.6
*
* Port Usage : Storage configuration
* Ports 1-36: 100GbE Controller and Shelf Storage Ports
*****
*****
```

5. Verify that the RCF 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.

6. Reapply any previous customizations to the switch configuration. Refer to [Review cabling and configuration considerations](#) for details of any further changes required.
7. After you verify the RCF versions and switch settings are correct, copy the running-config file to the startup-config file:

```
copy running-config startup-config
```

Show example

```
cs1# copy running-config startup-config
[#####] 100% Copy complete
```

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

[OS Command Reference.](#)

8. Reboot switch cs1.

```
cs1# reload
```

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

9. Repeat steps 1 through 7 on switch cs2.
10. Connect the cluster ports of all nodes in the ONTAP cluster to switches cs1 and cs2.

Step 2: Verify the switch connections

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

```
show interface brief
```

Show example

```
cs1# show interface brief | grep up
mgmt0  --                up      <mgmt ip address>
1000   1500
Eth1/11      1          eth  trunk  up      none
100G(D)  --
Eth1/12      1          eth  trunk  up      none
100G(D)  --
Eth1/13      1          eth  trunk  up      none
100G(D)  --
Eth1/14      1          eth  trunk  up      none
100G(D)  --
Eth1/15      1          eth  trunk  up      none
100G(D)  --
Eth1/16      1          eth  trunk  up      none
100G(D)  --
Eth1/17      1          eth  trunk  up      none
100G(D)  --
Eth1/18      1          eth  trunk  up      none
100G(D)  --
Eth1/23      1          eth  trunk  up      none
100G(D)  --
Eth1/24      1          eth  trunk  up      none
100G(D)  --
Eth1/25      1          eth  trunk  up      none
100G(D)  --
Eth1/26      1          eth  trunk  up      none
100G(D)  --
Eth1/27      1          eth  trunk  up      none
100G(D)  --
Eth1/28      1          eth  trunk  up      none
100G(D)  --
Eth1/29      1          eth  trunk  up      none
100G(D)  --
Eth1/30      1          eth  trunk  up      none
100G(D)  --
```

2. Verify that the cluster nodes are in their correct cluster VLANs using the following commands:

```
show vlan brief
```

```
show interface trunk
```


Show example

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Po999
30	VLAN0030	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9, Eth1/10, Eth1/11 Eth1/12, Eth1/13, Eth1/14 Eth1/15, Eth1/16, Eth1/17 Eth1/18, Eth1/19, Eth1/20 Eth1/21, Eth1/22, Eth1/23 Eth1/24, Eth1/25, Eth1/26 Eth1/27, Eth1/28, Eth1/29 Eth1/30, Eth1/31, Eth1/32 Eth1/33, Eth1/34, Eth1/35 Eth1/36

```
cs1# show interface trunk
```

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--

```

Eth1/9      1      trunking  --
Eth1/10     1      trunking  --
Eth1/11     1      trunking  --
Eth1/12     1      trunking  --
Eth1/13     1      trunking  --
Eth1/14     1      trunking  --
Eth1/15     1      trunking  --
Eth1/16     1      trunking  --
Eth1/17     1      trunking  --
Eth1/18     1      trunking  --
Eth1/19     1      trunking  --
Eth1/20     1      trunking  --
Eth1/21     1      trunking  --
Eth1/22     1      trunking  --
Eth1/23     1      trunking  --
Eth1/24     1      trunking  --
Eth1/25     1      trunking  --
Eth1/26     1      trunking  --
Eth1/27     1      trunking  --
Eth1/28     1      trunking  --
Eth1/29     1      trunking  --
Eth1/30     1      trunking  --
Eth1/31     1      trunking  --
Eth1/32     1      trunking  --
Eth1/33     1      trunking  --
Eth1/34     1      trunking  --
Eth1/35     1      trunking  --
Eth1/36     1      trunking  --

```

```

-----
-----

```

```

Port          Vlans Allowed on Trunk
-----

```

```

Eth1/1      30
Eth1/2      30
Eth1/3      30
Eth1/4      30
Eth1/5      30
Eth1/6      30
Eth1/7      30
Eth1/8      30
Eth1/9      30
Eth1/10     30
Eth1/11     30
Eth1/12     30

```

```
Eth1/13      30
Eth1/14      30
Eth1/15      30
Eth1/16      30
Eth1/17      30
Eth1/18      30
Eth1/19      30
Eth1/20      30
Eth1/21      30
Eth1/22      30
Eth1/23      30
Eth1/24      30
Eth1/25      30
Eth1/26      30
Eth1/27      30
Eth1/28      30
Eth1/29      30
Eth1/30      30
Eth1/31      30
Eth1/32      30
Eth1/33      30
Eth1/34      30
Eth1/35      30
Eth1/36      30
```

```
-----
-----
Port          Vlans Err-disabled on Trunk
-----
```

```
-----
Eth1/1        none
Eth1/2        none
Eth1/3        none
Eth1/4        none
Eth1/5        none
Eth1/6        none
Eth1/7        none
Eth1/8        none
Eth1/9        none
Eth1/10       none
Eth1/11       none
Eth1/12       none
Eth1/13       none
Eth1/14       none
Eth1/15       none
Eth1/16       none
```

Eth1/17	none
Eth1/18	none
Eth1/19	none
Eth1/20	none
Eth1/21	none
Eth1/22	none
Eth1/23	none
Eth1/24	none
Eth1/25	none
Eth1/26	none
Eth1/27	none
Eth1/28	none
Eth1/29	none
Eth1/30	none
Eth1/31	none
Eth1/32	none
Eth1/33	none
Eth1/34	none
Eth1/35	none
Eth1/36	none

Port STP Forwarding

Eth1/1	none
Eth1/2	none
Eth1/3	none
Eth1/4	none
Eth1/5	none
Eth1/6	none
Eth1/7	none
Eth1/8	none
Eth1/9	none
Eth1/10	none
Eth1/11	30
Eth1/12	30
Eth1/13	30
Eth1/14	30
Eth1/15	30
Eth1/16	30
Eth1/17	30
Eth1/18	30
Eth1/19	none
Eth1/20	none

```
Eth1/21      none
Eth1/22      none
Eth1/23      30
Eth1/24      30
Eth1/25      30
Eth1/26      30
Eth1/27      30
Eth1/28      30
Eth1/29      30
Eth1/30      30
Eth1/31      none
Eth1/32      none
Eth1/33      none
Eth1/34      none
Eth1/35      none
Eth1/36      none
```

```
-----
-----
Port          Vlans in spanning tree forwarding state and not pruned
-----
-----
```

```
Eth1/1      Feature VTP is not enabled
none
Eth1/2      Feature VTP is not enabled
none
Eth1/3      Feature VTP is not enabled
none
Eth1/4      Feature VTP is not enabled
none
Eth1/5      Feature VTP is not enabled
none
Eth1/6      Feature VTP is not enabled
none
Eth1/7      Feature VTP is not enabled
none
Eth1/8      Feature VTP is not enabled
none
Eth1/9      Feature VTP is not enabled
none
Eth1/10     Feature VTP is not enabled
none
Eth1/11     Feature VTP is not enabled
30
Eth1/12     Feature VTP is not enabled
30
```

```
Eth1/13      Feature VTP is not enabled
30
Eth1/14      Feature VTP is not enabled
30
Eth1/15      Feature VTP is not enabled
30
Eth1/16      Feature VTP is not enabled
30
Eth1/17      Feature VTP is not enabled
30
Eth1/18      Feature VTP is not enabled
30
Eth1/19      Feature VTP is not enabled
none
Eth1/20      Feature VTP is not enabled
none
Eth1/21      Feature VTP is not enabled
none
Eth1/22      Feature VTP is not enabled
none
Eth1/23      Feature VTP is not enabled
30
Eth1/24      Feature VTP is not enabled
30
Eth1/25      Feature VTP is not enabled
30
Eth1/26      Feature VTP is not enabled
30
Eth1/27      Feature VTP is not enabled
30
Eth1/28      Feature VTP is not enabled
30
Eth1/29      Feature VTP is not enabled
30
Eth1/30      Feature VTP is not enabled
30
Eth1/31      Feature VTP is not enabled
none
Eth1/32      Feature VTP is not enabled
none
Eth1/33      Feature VTP is not enabled
none
Eth1/34      Feature VTP is not enabled
none
Eth1/35      Feature VTP is not enabled
none
```

```
Eth1/36      Feature VTP is not enabled
none
```



For specific port and VLAN usage details, refer to the banner and important notes section in your RCF.

Step 3: Set up your ONTAP cluster

NetApp recommends that you use System Manager to set up new clusters.

System Manager provides a simple and easy workflow for cluster setup and configuration including assigning a node management IP address, initializing the cluster, creating a local tier, configuring protocols and provisioning initial storage.

Go to [Configure ONTAP on a new cluster with System Manager](#) for setup instructions.

What's next?

[Configure switch health monitoring.](#)

Replace a Cisco Nexus 9336C-FX2 storage switch

You can replace a defective Nexus 9336C-FX2 switch in a cluster network. This is a nondisruptive procedure.

What you'll need

Before installing the NX-OS software and RCFs on a Cisco Nexus 9336C-FX2 storage switch, ensure that:

- Your system can support Cisco Nexus 9336C-FX2 storage switches.
- You have consulted the switch compatibility table on the Cisco Ethernet Switch page for the supported ONTAP, NX-OS, and RCF versions.
- You have referred to the appropriate software and upgrade guides available on the Cisco web site.

Cisco Nexus 3000 Series Switches:

- You have downloaded the applicable RCFs.
- The existing network configuration has 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.
- The replacement Cisco Nexus 9336C-FX2 switch has the following characteristics:
 - Management network connectivity is functional.
 - Console access to the replacement switch is in place.
 - The appropriate RCF and NX-OS operating system image is loaded onto the switch.
 - Initial configuration of the switch is complete.

About this task

This procedure replaces the second Nexus 9336C-FX2 storage switch S2 with the new 9336C-FX 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.



There can be dependencies between command syntax in the RCF and NX-OS versions.

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
```

Show example

```
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
```


Show example

```
storage::*> network device-discovery show
Node/          Local Discovered
Protocol      Port  Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
      e3a  S1                Ethernet1/1  NX9336C
      e4a  node2             e4a          AFF-A700
      e4e  node2             e4e          AFF-A700
node1/lldp
      e3a  S1                Ethernet1/1  -
      e4a  node2             e4a          -
      e4e  node2             e4e          -
node2/cdp
      e3a  S1                Ethernet1/2  NX9336C
      e4a  node1             e4a          AFF-A700
      e4e  node1             e4e          AFF-A700
node2/lldp
      e3a  S1                Ethernet1/2  -
      e4a  node1             e4a          -
      e4e  node1             e4e          -
storage::*>
```

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

```
show lldp neighbors
```

Show example

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID          Local Intf  Hold-time  Capability  Port ID
node1               Eth1/1     121        S           e3a
node2               Eth1/2     121        S           e3a
SHFGD2008000011    Eth1/5     121        S           e0a
SHFGD2008000011    Eth1/6     120        S           e0a
SHFGD2008000022    Eth1/7     120        S           e0a
SHFGD2008000022    Eth1/8     120        S           e0a
```

5. Verify the shelf ports in the storage system:

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

Show example

```
storage::*> storage shelf port show -fields remote-device,remote-  
port  
shelf   id  remote-port  remote-device  
----- --  -  
3.20    0  Ethernet1/5  S1  
3.20    1  -            -  
3.20    2  Ethernet1/6  S1  
3.20    3  -            -  
3.30    0  Ethernet1/7  S1  
3.20    1  -            -  
3.30    2  Ethernet1/8  S1  
3.20    3  -            -  
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
```

Show example

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

9. Verify that both switches are available:

```
network device-discovery show
```

Show example

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e3a  S1                        Ethernet1/1 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
```

Show example

```
storage::*> storage shelf port show -fields remote-device,remote-  
port  
shelf    id    remote-port    remote-device  
-----  --    -  
3.20    0    Ethernet1/5    S1  
3.20    1    Ethernet1/5    NS2  
3.20    2    Ethernet1/6    S1  
3.20    3    Ethernet1/6    NS2  
3.30    0    Ethernet1/7    S1  
3.20    1    Ethernet1/7    NS2  
3.30    2    Ethernet1/8    S1  
3.20    3    Ethernet1/8    NS2  
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
```

What's next?

[Configure switch health monitoring.](#)

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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