Storage switches

Install and maintain

NetApp
February 20, 2026

Table of Contents

Storage switches

Cisco Nexus 9336C-FX2 or 9336C-FX2-T

Get started

Installation and setup workflow for Cisco Nexus 9336C-FX2 9336C-FX2-T storage switches

The Cisco Nexus 9336C-FX2 and 9336C-FX2-T switches are part of the Cisco Nexus 9000 platform and can be installed in a NetApp system cabinet.

Cisco Nexus 9336C-FX2 (36 ports) is high-port density cluster/storage/data switch. Cisco Nexus 9336C-FX2-T (12 ports) is a low-port-density, high performance switch that supports 10/25/40/100GbE configurations.

Follow these workflow steps to install and setup your to Cisco 9336C-FX2 and 9336C-FX2-T switches.

Review the configuration requirements

Review the configuration requirements for the 9336C-FX2 and 9336C-FX2-T storage switches.

Review the components and part numbers

Review the components and part numbers for the 9336C-FX2 and 9336C-FX2-T storage switches.

Review the required documentation

Review specific switch and controller documentation to set up your 9336C-FX2 and 9336C-FX2-T switches and the ONTAP cluster.

Review the Smart Call Home requirements

Review the requirements for the Cisco Smart Call Home feature, used to monitor the hardware and software components on your network.

Install the hardware

Install the switch hardware.

Configure the software

Configure the switch software.

Configuration requirements for Cisco Nexus 9336C-FX2 and 9336C-FX2-T storage switches

For Cisco Nexus 9336C-FX2 and 9336C-FX2-T switches installation and maintenance, make sure to review configuration and network requirements.

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.

What's next

After you've reviewed the configuration requirements, you can confirm your components and part numbers.

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

For Cisco Nexus 9336C-FX2 and 9336C-FX2-T storage 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 and 9336C-FX2-T storage switches, fans, and power supplies:

Part number	Description
X190200-CS-PE	Cluster Switch, N9336C 36Pt PTSX 10/25/40/100G
X190200-CS-PI	Cluster Switch, N9336C 36Pt PSIN 10/25/40/100G
X190212-CS-PE	Cluster Switch, N9336C 12Pt (9336C-FX2-T) PTSX 10/25/40/100G
X190212-CS-PI	Cluster Switch, N9336C 12Pt (9336C-FX2-T) PSIN 10/25/40/100G
SW-N9K-FX2-24P-UPG	SW, Cisco 9336CFX2 24-Port POD License
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100GQSFP28
X190002	Accessory Kit X190001/X190003

Part number	Description
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

Cisco Smart licenses for 9336C-FX2-T ports only

In order to activate more than 12 ports on your Cisco Nexus 9336C-FX-T storage switch, you must purchase a Cisco Smart license. Cisco Smart licenses are managed through Cisco Smart accounts.

1. Create a new Smart account, if required. See Create a new Smart account for details.
2. Request access to an existing Smart account. See Request access to an existing Smart account for details.

> Once you have purchased your Smart license, install the appropriate RCF to enable and configure all 36 available ports for use.

What's next

After you've confirmed your components and part numbers, you can review the required documentation.

Documentation requirements for Cisco Nexus 9336C-FX2 and 9336C-FX2-T storage switches

For Cisco Nexus 9336C-FX2 and 9336C-FX2-T switch installation and maintenance, make 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
Nexus 9000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 9000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.

Document title	Description
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 9000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 9000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 9000 switches.
Nexus 9000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 9000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 9000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 9000 Series.
Regulatory Compliance and Safety Information for Cisco Nexus 9000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 9000 series switches.

ONTAP systems documentation

To set up an ONTAP system, you need the following documents for your version of the operating system from ONTAP 9.

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

Rail kit and cabinet documentation

To install a Cisco 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.

Name	Description
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, 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.

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.

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.

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

- 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 the hardware

Hardware install workflow for Cisco Nexus 9336C-FX2 and 9336C-FX2-T storage switches

To install and configure the hardware for 9336C-FX2 and 9336C-FX2-T storage switches, follow these steps:

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.

Install the switch

Install the 9336C-FX2 and 9336C-FX2-T storage switches.

3 Install the switch in a NetApp cabinet

Install the 9336C-FX2 and 9336C-FX2-T switches and pass-through panel in a NetApp cabinet as required.

4 Review cabling and configuration considerations

Before configuring your 9336C-FX2 and 9336C-FX2-T switches, review the cabling and configuration considerations.

Complete the Cisco Nexus 9336C-FX2 or 9336C-FX2-T 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.

- 9336C-FX2 sample cabling worksheet
- 9336C-FX2 blank cabling worksheet
- 9336C-FX2-T sample cabling worksheet (12-port)
- 9336C-FX2-T blank cabling worksheet (12-port)

9336C-FX2 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

Cluster switch A		Cluster switch B	
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	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

Cluster switch A		Cluster switch B	
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

9336C-FX2 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	

Cluster switch A		Cluster switch B	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	

Cluster switch A		Cluster switch B	
35		35	
36		36	

9336C-FX2-T sample cabling worksheet (12-port)

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 though 36	Requires license	11 through 36	Requires license

9336C-FX2-T blank cabling worksheet (12-port)

You can use the blank cabling worksheet to document the platforms that are supported as nodes in a cluster.

Cluster switch A		Cluster switch B	
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 through 36	Requires license	11 through 36	Requires license

See the Hardware Universe for more information on switch ports.

What's next

After you've completed your cabling worksheets, you can install the switch.

Install the 9336C-FX2 and 9336C-FX2-T storage switches

Follow this procedure to install Cisco Nexus 9336C-FX2 and 9336C-FX2-T storage switches.

Before you begin

Make sure you have the following:

- 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 storage network and management network RCFs downloaded from the NetApp Support Site at mysupport.netapp.com.

  All Cisco storage 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 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 network and management network switches to the controllers using the completed cabling worksheets.
3. Power on the network and management network switches and controllers.

What's next?

Optionally, you can install a Cisco Nexus 9336C-FX2 switch in a NetApp cabinet. Otherwise, go to configure the switch.

Install Cisco Nexus 9336C-FX2 and 9336C-FX2-T switches in a NetApp cabinet

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

Before you begin

Make sure you have the following:

- 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

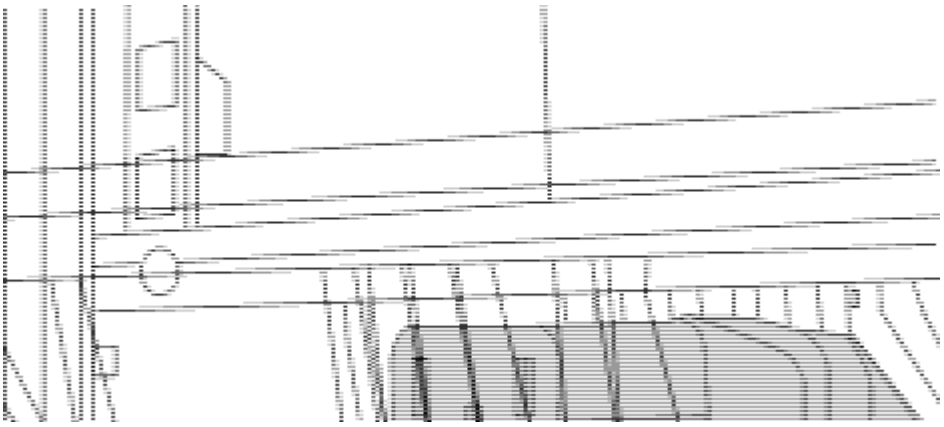
a. Determine the vertical location of the switches and blanking panel in the cabinet.

   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.

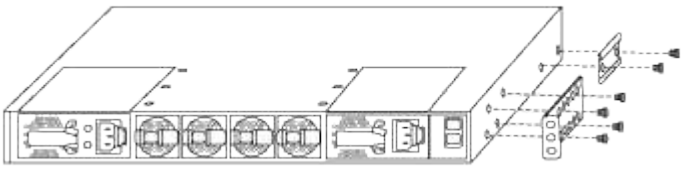
d. Insert the female connectors of both 48-inch jumper cords from the rear of the panel and through the brush assembly.



(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.

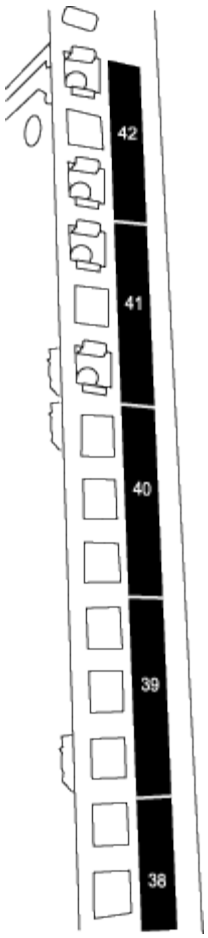


   b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.

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

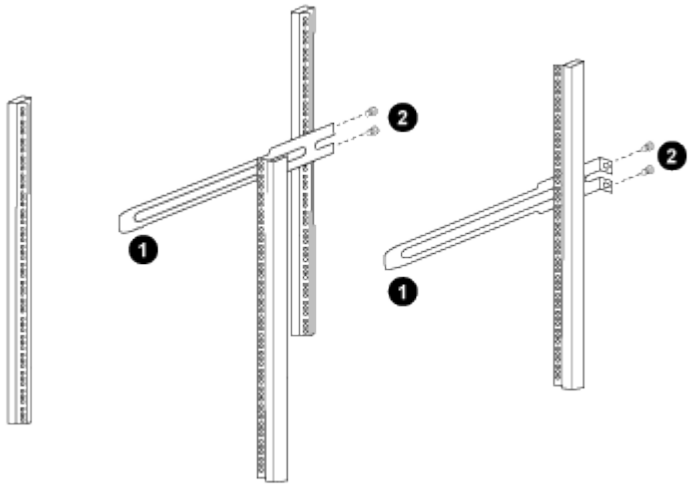
   d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.

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.

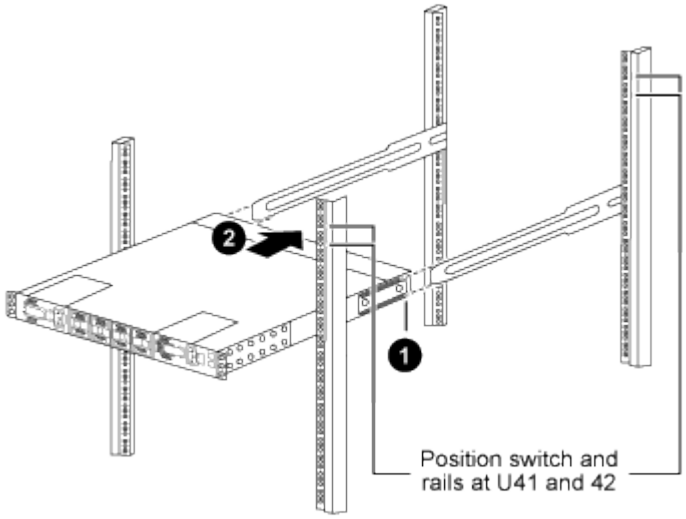
   b. Repeat step 4a for the right side rear post.

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.

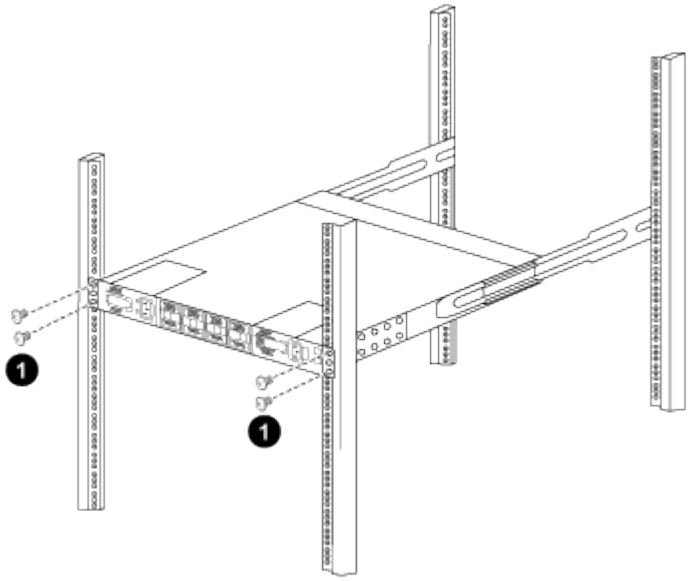
a. Position the back of the switch at RU41.



(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.

What's next

After you've installed the switches in the NetApp cabinet, you can configure the Cisco Nexus 9336C-FX2 and 9336C-FX2-T switches.

Review cabling and configuration considerations

Before configuring your 9336C-FX2 and 9336C-FX2-T switches, review the cabling and configuration requirements.

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

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

```
(s1)(config)# interface Ethernet1/19
For 100GbE speed:
(s1)(config-if)# speed 100000
For 40GbE speed:
(s1)(config-if)# speed 40000
(s1)(config-if)# no negotiate auto
(s1)(config-if)# exit
(s1)(config)# exit
Save the changes:
(s1)# copy running-config startup-config
```

Related information

- Refer to Hardware Universe for more information on switch ports.
- See What additional information do I need to install my equipment that is not in HWU? for more information about switch installation requirements.

Configure the software

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

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

1. **Configure the switch**

Configure the 9336C-FX2 and 9336C-FX2-T storage switches.

2. **Prepare to install the NX-OS software and RCF**

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

3. **Install or upgrade the NX-OS software**

Download and install or upgrade the NX-OS software on the Cisco 9336C-FX2 and 9336C-FX2-T storage switches.

4. **Install or upgrade the RCF**

Install or upgrade the RCF after setting up the Cisco 9336C-FX2 and 9336C-FX2-T switches for the first time. You can also use this procedure to upgrade your RCF version.

5. **Verify SSH configuration**

Verify that SSH is enabled on the switches to use the Ethernet Switch Health Monitor (CSHM) and log collection features.

6. **Reset the switch to factory defaults**

Erase the 9336C-FX2 and 9336C-FX2-T storage switches settings.

Configure the 9336C-FX2 and 9336C-FX2-T storage switches

Follow this procedure to configure the Cisco Nexus 9336C-FX2 and 9336C-FX2-T switches.

Before you begin

Make sure you have the following:

- 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 network and management network RCFs downloaded from the NetApp Support Site at mysupport.netapp.com. All Cisco 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 network switches.

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

Prompt	Response
Abort Auto Provisioning and continue with normal setup? (yes/no)	Respond with **yes**. The default is no.
Do you want to enforce secure password standard? (yes/no)	Respond with **yes**. The default is yes.
Enter the password for admin.	The default password is "admin"; you must create a new, strong password. A weak password can be rejected.
Would you like to enter the basic configuration dialog? (yes/no)	Respond with **yes** at the initial configuration of the switch.
Create another login account? (yes/no)	Your answer depends on your site's policies on alternate administrators. The default is **no**.
Configure read-only SNMP community string? (yes/no)	Respond with **no**. The default is no.
Configure read-write SNMP community string? (yes/no)	Respond with **no**. The default is no.
Enter the switch name.	The switch name is limited to 63 alphanumeric characters.
Continue with Out-of-band (mgmt0) management configuration? (yes/no)	Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip_address.
Configure the default-gateway? (yes/no)	Respond with **yes**. At the IPv4 address of the default-gateway: prompt, enter your default_gateway.
Configure advanced IP options? (yes/no)	Respond with **no**. The default is no.

Prompt	Response
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 Ethernet Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.
Enter the type of SSH key you want to generate (dsa/rsa/rsa1).	The default is **rsa**.
Enter the number of key bits (1024-2048).	Enter the number of key bits from 1024 to 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.

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 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?

After you've configured your switches, you can prepare to install the NX-OS software and RCF.

Prepare to install or upgrade 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 s1 and s2.
- The node names are cluster1-01 and cluster1-02.

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, suppress automatic case creation by invoking an AutoSupport message:
   `system node autosupport invoke -node * -type all -message MAINT=xh`

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

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

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

   ```
   set -privilege advanced
   ```

   The advanced prompt (`*>`) appears.

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

   ```
   network device-discovery show -protocol lldp
   ```

Show example

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/lldp
            e5a    s1                        Eth1/2            N9K-
C9336C
            e3b    s2                        Eth1/2            N9K-
C9336C
cluster1-01/lldp
            e5a    s1                        Eth1/1            N9K-
C9336C
            e3b    s2                        Eth1/1            N9K-
C9336C
.
.
```

4. Check the administrative or operational status of each node storage port and storage shelf port.
   a. Display the node storage port attributes:

```
storage port show
```

Show example

```
cluster1::*> storage port show
Speed                      VLAN
Node           Port Type   Mode    (Gb/s) State    Status      ID
-------------- ---- ------ ------- ------ -------- --------- ----
cluster1-01
               e5a  ENET   storage    100 enabled  online      -
               e3b  ENET   storage    100 enabled  online      -
cluster1-02

               e5a  ENET   storage    100 enabled  online      -
               e3b  ENET   storage    100 enabled  online      -

.
.
```

b. Display the storage shelf port attributes:

```
storage shelf port show
```

Show example

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

Shelf ID Module State        Internal?
-------- -- ------ ------------ ---------
1.4
         0 A      connected    false
         1 A      connected    false
         2 B      connected    false
         3 B      connected    false
.
.
```

c. Verify that switch health monitoring (CSHM) is enabled for the switch so that the switches are monitored:

```
system switch ethernet show
```

Show example

```
cluster1::> system switch ethernet show
  Switch            Type               Address          Model
  ----------------- ------------------ ---------------
---------------
  s1                storage-network    1.2.3.4          N9K-
C9336C-FX2
     Serial Number: FFFXXXXXXX1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2                storage-network    2.3.4.5          N9K-
C9336C-FX2
     Serial Number: FEEXXXXXXX2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

What's next?

After you've prepared to install the NX-OS software and RCF, you can install or upgrade the NX-OS software.

Install or upgrade the NX-OS software

Follow this procedure to install or upgrade the NX-OS software on the Nexus 9336C-FX2 and 9336C-FX2-T switches.

Before you begin, complete the procedure in Prepare to install NX-OS and RCF.

Review requirements

Before you begin

Make sure you have the following:

- 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 s1 and s2.
- The node names are cluster1-01 and cluster1-02.

Install or upgrade 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 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:

   ```
   s2# ping 172.19.2.1 VRF management
   Pinging 172.19.2.1 with 0 bytes of data:

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

3. If you are setting up your switch for the first time, skip to step 5. If you are upgrading your switch, proceed to the next step.
4. Check the administrative or operational status of each node storage port and storage shelf port.
   a. Display the node storage port attributes:

      ```
      storage port show
      ```

Show example

```
cluster1::*> storage port show
Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status      ID
-------------- ---- ----- ------- ------ -------- --------- ----
cluster1-01
               e5a  ENET  storage    100 enabled  online      -
               e3b  ENET  storage    100 enabled  online      -
cluster1-02

               e5a  ENET  storage    100 enabled  online      -
               e3b  ENET  storage    100 enabled  online      -
.
.
```

b. Display the storage shelf port attributes:

```
storage shelf port show
```

Show example

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

Shelf ID Module State        Internal?
----- -- ------ ------------ ---------
1.4
       0 A      connected    false
       1 A      connected    false
       2 B      connected    false
       3 B      connected    false
.
.
```

c. Verify that switch health monitoring (CSHM) is enabled for the switch so that the switches are monitored:

```
system switch ethernet show
```

Show example

```
cluster1::> system switch ethernet show
  Switch            Type               Address          Model
  ----------------- ------------------ ---------------
---------------
  s1                storage-network    1.2.3.4          N9K-
C9336C-FX2
     Serial Number: FFFXXXXXXX1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2                storage-network    2.3.4.5          N9K-
C9336C-FX2
     Serial Number: FFFXXXXXXX2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

5. Log in to the switch using SSH or by using a serial console.
6. Copy the NX-OS software and EPLD images to the Nexus 9336C-FX2 switch.

Show example

```
s2# 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.


s2# 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

```
s2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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


Hardware
  cisco 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: s2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

8. Install the NX-OS image.

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

Show example

```
s2# 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

```
s2# show version

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

Software
  BIOS: version 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: s2
  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

```
s2# 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

s2# install epld bootflash:n9000-epld.9.3.5.img module all
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 reboots, log in again and verify that the new version of EPLD loaded successfully.

Show example

```
s2# 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. If you are setting up your switch for the first time, skip to step 14. If you are upgrading your switch, proceed to the next step.
13. Verify the health status of each node storage port and storage shelf port.
    a. Display the node storage port attributes:

```
storage port show
```

Show example

```
cluster1::*> storage port show
Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status      ID
-------------- ---- ----- ------- ------ -------- --------- ----
cluster1-01
               e5a  ENET  storage    100 enabled  online      -
               e3b  ENET  storage    100 enabled  online      -
cluster1-02

               e5a  ENET  storage    100 enabled  online      -
               e3b  ENET  storage    100 enabled  online      -
.
.
```

    b. Display the storage shelf port attributes:

```
storage shelf port show
```

Show example

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

Shelf ID Module State        Internal?
----- -- ------ ------------ ---------
1.4
       0 A      connected    false
       1 A      connected    false
       2 B      connected    false
       3 B      connected    false
.
.
```

c. Verify that switch health monitoring (CSHM) is enabled for the switches so that they are monitored:

```
system switch ethernet show
```

Show example

```
cluster1::> system switch ethernet show
  Switch            Type               Address          Model
  ----------------- ------------------ ---------------
---------------
  s1                storage-network    1.2.3.4          N9K-
C9336C-FX2
     Serial Number: FFFXXXXXXX1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2                storage-network    2.3.4.5          N9K-
C9336C-FX2
     Serial Number: FFFXXXXXXX2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

14. Repeat steps 5 to 13 to install the NX-OS software on switch s1.

What's next?

After you've installed or upgraded the NX-OS software, you can install or upgrade the RCF.

Install or upgrade the RCF

Install or upgrade the Reference Configuration File (RCF) overview

You install the Reference Configuration File (RCF) after setting up the Nexus 9336C-FX2 storage switch for the first time. You upgrade your RCF version when you have an existing version of the RCF file installed on your switch.

See the Knowledge Base article How to clear configuration on a Cisco interconnect switch while retaining remote connectivity for further information when installing or upgrading your RCF.

Available RCF configuration

Storage - (Storage RCF 1.*xx*) is the available RCF configuration where all ports are configured for 100GbE NVMe storage connections.

Suggested documentation

- Cisco Ethernet Switches

  Consult the switch compatibility table for the supported ONTAP and RCF versions on the NetApp Support Site. Note that there can be command dependencies between the command syntax in the RCF and the syntax found in specific versions of NX-OS.

- Cisco Nexus 9000 Series Switches

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

About the examples

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

- The names of the two Cisco switches are s1 and s2.
- The node names are cluster1-01 and cluster1-02.

See the Hardware Universe to verify the correct ports on your platform.

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

Commands used

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

What's next?

After you've reviewed the install RCF or upgrade RCF procedure, you can install the RCF or upgrade your RCF as needed.

Install the Reference Configuration File

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

See the Knowledge Base article How to clear configuration on a Cisco interconnect switch while retaining remote connectivity for further information when installing your RCF.

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 s1 and switch s2 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 storage ports and storage shelf ports are not connected.

Step 1: Install the RCF on the switches

1. Log in to switch s2 using SSH or by using a serial console.

2. Copy the RCF to the bootflash of switch s2 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 s2:

   ```
   s2# copy tftp: bootflash: vrf management
   Enter source filename: NX9336C-FX2-RCF-v1.13-1-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 `NX9336C-FX2-RCF-v1.13-1-Storage.txt` being installed on switch s2:

   ```
   s2# copy NX9336C-FX2-RCF-v1.13-1-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

```
s2# show banner motd

*****************************************************
* NetApp Reference Configuration File (RCF)
*
* Switch    : NX9336C-FX2
* Filename  : NX9336C-FX2-RCF-v1.13-1-Storage.txt
* Date      : 05-22-2025
* Version   : v1.13
*
* Port Usage : Storage configuration
* Ports  1-36: 100GbE Controller and Shelf Storage Ports
*
* IMPORTANT NOTES
*
* Interface port-channel999 is reserved to identify the version of
this file.
*****************************************************
```

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. Record any custom additions between the current `running-config` file and the RCF file in use.
7. After you verify that the RCF versions and switch settings are correct, copy the `running-config` file to the `startup-config` file.

   ```
   s2# copy running-config startup-config
   [########################################] 100% Copy complete
   ```

8. Reboot switch s2.

   `s2# **reload**`

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

9. Repeat steps 1 through 8 on switch s1.
10. Connect the node storage ports and storage shelf ports of all the nodes in the ONTAP cluster to switches s1 and s2.

Step 2: Verify the switch connections

1. Verify that the switch ports are **up**.

```
show interface brief
```

Show example

```
s1# 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 node storage ports and storage shelf ports are in their correct VLANs using the following commands:

   `show vlan brief`

   `show interface trunk`

Show example

```
s1# 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

s1# show interface trunk

----------------------------------------------------
Port          Native  Status        Port
              Vlan                  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?

After you've installed your RCF, you can verify the SSH configuration

Upgrade your Reference Configuration File (RCF)

You upgrade your RCF version when you have an existing version of the RCF file installed on your operational switches.

Before you begin

Make sure you have the following:

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs or similar issues).
- The current RCF.
- If you are updating your RCF version, you need a boot configuration in the RCF that reflects the desired boot images.

  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.

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 or have preserved basic configuration information before erasing the switch settings.

Step 1: Prepare for the upgrade

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

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

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

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

   ```
   set -privilege advanced
   ```

   The advanced prompt (*>) appears.

3. Display the ports on each node that are connected to the 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
               e5a    s1                      Ethernet1/7     N9K-
   C9336C
               e3b    s2                      Ethernet1/7     N9K-
   C9336C
   cluster1-02/cdp
               e5a    s1                      Ethernet1/8     N9K-
   C9336C
               e3b    s2                      Ethernet1/8     N9K-
   C9336C
   .
   .
   .
   ```

4. Check the administrative or operational status of each node storage port and storage shelf port.
   a. Verify that all the node storage ports are up with a healthy status:

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

Show example

```
cluster1::*> storage port show -port-type ENET


                                      Speed
Node               Port Type  Mode    (Gb/s) State    Status
------------------ ---- ----- ------- ------ -------- -----------
cluster1-01
                   e5a ENET  -         100   enabled  online
                   e3b ENET  -         100   enabled  online
cluster1-02
                   e5a ENET  -         100   enabled  online
                   e3b ENET  -         100   enabled  online
.
.
```

b. Verify that all the storage shelf ports are up with a healthy status:

```
storage shelf port show
```

Show example

```
cluster1::> storage shelf port show

Shelf ID Module State        Internal?
-------- -- ------ ------------ ---------
1.4
       0 A      connected    false
       1 A      connected    false
       2 B      connected    false
       3 B      connected    false
.
.
```

c. Verify that the switches are being monitored.

```
system switch ethernet show
```

Show example

```
cluster1::*> system switch ethernet show
  Switch            Type               Address          Model
  ----------------- ------------------ ---------------
---------------
  s1                storage-network    1.2.3.4          N9K-
C9336C-FX2
     Serial Number: FFFXXXXXXX1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2                storage-network    2.3.4.5          N9K-
C9336C-FX2
     Serial Number: FEEXXXXXXX2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

Step 2: Upgrade the RCF

1. Log in to the switch s2 using SSH or by using a serial console.
2. Shut down the ports connected to all the ports of the nodes.

```
s2> enable
s2# configure
s2(config)# interface e1/1-36
s2(config-if-range)# shutdown
s2(config-if-range)# exit
s2(config)# exit
```

Make sure to shutdown **all** connected ports to avoid any network connection issues. See the Knowledge Base article Node out of quorum when migrating cluster LIF during switch OS upgrade for further details.

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

```
show running-config
```

a. Record any custom additions between the current `running-config` and the RCF file in use (such as an SNMP configuration for your organization).

b. For NX-OS 10.2 and later, use the `show diff running-config` command to compare with the saved RCF file in the bootflash. Otherwise, use a third-party diff or compare tool.

4. Save basic configuration details to the `write_erase.cfg` file on the bootflash.

Make sure to configure the following:

- Username and password
- Management IP address
- Default gateway
- Switch name

```
s2# show run | i "username admin password" > bootflash:write_erase.cfg

s2# show run | section "vrf context management" >> bootflash:write_erase.cfg

s2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

s2# show run | section "switchname" >> bootflash:write_erase.cfg
```

See the Knowledge Base article How to clear configuration on a Cisco interconnect switch while retaining remote connectivity for further details.

5. Verify that the `write_erase.cfg` file is populated as expected:

```
show file bootflash:write_erase.cfg
```

6. Issue the `write erase` command to erase the current saved configuration:

```
s2# write erase

Warning: This command will erase the startup-configuration.

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

7. Copy the previously saved basic configuration into the startup configuration.

```
s2# copy bootflash:write_erase.cfg startup-config
```

8. Reboot the switch:

```
s2# reload

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

9. After the management IP address is reachable again, log in to the switch through SSH.

You might need to update host file entries related to the SSH keys.

10. Copy the RCF to the bootflash of switch s2 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.

    Show example

    This example shows TFTP being used to copy an RCF to the bootflash on switch s2:

    ```
    s2# copy tftp: bootflash: vrf management
    Enter source filename: NX9336C-FX2-RCF-v1.13-1-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)...
    ```

11. 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 `NX9336C-FX2-RCF-v1.13-1-Storage.txt` being installed on switch s2:

    ```
    s2# copy NX9336C-FX2-RCF-v1.13-1-Storage.txt running-config echo-commands
    ```

    Make sure to thoroughly read the **Installation notes**, **Important Notes**, and **banner** sections of your RCF. You must read and follow these instructions to ensure the proper configuration and operation of the switch.

12. Verify that the RCF file is the correct newer version:

    ```
    show running-config
    ```

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

    - The RCF banner
    - The node and port settings
    - Customizations

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

13. Reapply any previous customizations to the switch configuration.
14. After you verify the RCF versions, custom additions, 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.

    ```
    s2# copy running-config startup-config

    [] 100% Copy complete
    ```

15. Reboot switch s2. You can ignore the “cluster switch health monitor” alerts and “cluster ports down” events reported on the nodes while the switch reboots.

    ```
    s2# reload

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

16. Check the administrative or operational status of each node storage port and storage shelf port.
    a. Verify that all the storage ports are up with a healthy status:

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

    Show example

    ```
    cluster1::*> storage port show -port-type ENET


                                         Speed
    Node                Port Type  Mode    (Gb/s) State    Status
    ------------------- ---- ----- ------- ------ -------- -----------
    cluster1-01
                        e5a  ENET  -          100 enabled  online
                        e3b  ENET  -          100 enabled  online
    cluster1-02
                        e5a  ENET  -          100 enabled  online
                        e3b  ENET  -          100 enabled  online
    .
    .
    ```

    b. Verify that all the storage shelf ports are up with a healthy status:

    ```
    storage shelf port show
    ```

Show example

```
cluster1::> storage shelf port show

Shelf ID Module State        Internal?
----- -- ------ ------------ ---------
1.4
       0 A      connected    false
       1 A      connected    false
       2 B      connected    false
       3 B      connected    false
.
.
```

c. Verify that the switches are being monitored:

```
system switch ethernet show
```

Show example

```
cluster1::> system switch ethernet show
  Switch           Type               Address          Model
  ---------------- ------------------ ---------------
---------------
  s1               storage-network    1.2.3.4          N9K-
C9336C-FX2
     Serial Number: FFFXXXXXXX1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2               storage-network    2.3.4.5          N9K-
C9336C-FX2
     Serial Number: FEEXXXXXXX2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

17. Repeat steps 1 to 16 on switch s1.

Step 3: Verify the storage network

Complete the following steps on each storage switch to verify that the storage network is functioning properly after the RCF upgrade.

1. Verify that the switch ports connected to the node storage ports and storage shelf ports are **up**.

```
show interface brief
```

2. Verify that the expected node storage ports are still connected:

```
show cdp neighbors
```

3. Verify that the expected storage shelf ports are still connected:

```
show lldp neighbors
```

4. Verify that the node storage ports and storage shelf ports are in their correct VLANs using the following commands:

```
show vlan brief
```

```
show interface trunk
```

What's next?

After you've upgraded your RCF, you can verify the SSH configuration.

Verify your SSH configuration

If you are using the Ethernet Switch Health Monitor (CSHM) and log collection features, verify that SSH and SSH keys are enabled on the switches.

Steps

1. Verify that SSH is enabled:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Verify that the SSH keys are enabled:

```
show ssh key
```

Show example

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

When enabling FIPS, you must change the bitcount to 256 on the switch using the command `ssh key ecdsa 256 force`. See Configure network security using FIPS for more details.

What's next?

After you've verified your SSH configuration, you configure switch health monitoring.

Reset the 9336C-FX2 and 9336C-FX2-T storage switches to factory defaults

To reset the 9336C-FX2 and 9336C-FX2-T storage switches to factory defaults, you must erase the 9336C-FX2 and 9336C-FX2-T switch settings.

About this task

- You must be connected to the switch using the serial console.
- This task resets the configuration of the management network.

Steps

1. Erase the existing configuration:

   `write erase`

   ```
   (s2)# write erase

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

2. Reload the switch software:

   `reload`

   ```
   (s2)# reload

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

   The system reboots and enters the configuration wizard. During the boot, if you receive the prompt “Abort Auto Provisioning and continue with normal setup? (yes/no)[n]”, you should respond **yes** to proceed.

What’s next

After you’ve reset your switches, you can reconfigure them as needed.

Replace Cisco Nexus 9336C-FX2 and 9336C-FX2-T storage switches

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

Before you begin

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

- Your system can support Cisco Nexus 9336C-FX2 and 9336C-FX2-T 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.

- 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 cluster1-01 and cluster1-02.

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
                                  Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
cluster1-01
               e5a  ENET  storage 100    enabled  online      30
               e3b  ENET  storage   0    enabled  offline     30
cluster1-02
               e5a  ENET  storage 100    enabled  online      30
               e3b  ENET  storage   0    enabled  offline     30
.
.
```

3. Verify that storage switch s1 is available:

   `network device-discovery show`

Show example

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol   Port  Device (LLDP: ChassisID)  Interface  Platform
--------   ----  ----------------------   ---------   ---------
cluster1-01/cdp
           e5a   s1                       Ethernet1/1 NX9336C
           e4a   cluster1-02              e4a         AFF-A700
           e4e   cluster1-02              e4e         AFF-A700
cluster1-01/lldp
           e5a   s1                       Ethernet1/1 -
           e4a   cluster1-02              e4a         -
           e4e   cluster1-02              e4e         -
cluster1-02/cdp
           e3b   s1                       Ethernet1/2 NX9336C
           e4a   cluster1-01              e4a         AFF-A700
           e4e   cluster1-01              e4e         AFF-A700
cluster1-02/lldp
           e3b   s1                       Ethernet1/2 -
           e4a   cluster1-01              e4a         -
           e4e   cluster1-01              e4e         -
.
.
```

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

   `show lldp neighbors`

   Show example

```
S1# show lldp neighbors
Capability codes:
   (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
   (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID        Local Intf   Hold-time    Capability    Port ID
cluster1-01      Eth1/1       121          S             e5a
cluster1-02      Eth1/2       121          S             e5a
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 storage 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   -             -
.
.
```

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
                                     Speed                       VLAN
Node             Port Type  Mode    (Gb/s) State    Status       ID
---------------- ---- ----- ------- ------ -------- --------- ----
cluster1-01
                 e5a  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
cluster1-02
                 e5a  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
.
.
```

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
--------  ----  -----------------------   ---------   ---------
cluster1-01/cdp
          e3a  s1                         Ethernet1/1 NX9336C
          e4a  cluster1-02                e4a         AFF-A700
          e4e  cluster1-02                e4e         AFF-A700
          e7b  ns2                       Ethernet1/1 NX9336C
cluster1-01/lldp
          e3a  s1                         Ethernet1/1 -
          e4a  cluster1-02                e4a         -
          e4e  cluster1-02                e4e         -
          e7b  ns2                        Ethernet1/1 -
cluster1-02/cdp
          e3a  s1                         Ethernet1/2 NX9336C
          e4a  cluster1-01                e4a         AFF-A700
          e4e  cluster1-01                e4e         AFF-A700
          e7b  ns2                        Ethernet1/2 NX9336C
cluster1-02/lldp
          e3a  s1                         Ethernet1/2 -
          e4a  cluster1-01                e4a         -
          e4e  cluster1-01                e4e         -
          e7b  ns2                        Ethernet1/2 -
.
.
```

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?

After you've replaced your switches, you can configure switch health monitoring.

Cisco Nexus 3232C

Get started

Installation and setup workflow for Cisco Nexus 3232C storage switches

The Cisco Nexus 3232C switches are part of the Cisco Nexus 3000 platform and can be installed in a NetApp system cabinet.

Follow these workflow steps to install and setup your to Cisco 3232C switches.

Review the configuration requirements

Review the configuration requirements for the 3232C storage switches.

Review the required documentation

Review specific switch and controller documentation to set up your 3232C switches and the ONTAP cluster.

Review the Smart Call Home requirements

Review the requirements for the Cisco Smart Call Home feature, used to monitor the hardware and software components on your network.

4 Install the hardware

Install the switch hardware.

5 Configure the software

Configure the switch software.

Configuration requirements for Cisco Nexus 3232C storage switches

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

Configuration requirements

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

Network requirements

You need the following network information for all switch configurations:

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

Refer to the Hardware Universe for the latest information. See What additional information do I need to install my equipment that is not in HWU? for more information about switch installation requirements.

What's next

After you've confirmed your configuration requirements, you can review the required documentation.

Documentation requirements for Cisco Nexus 3232C storage switches

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

Switch documentation

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

Document title	Description
Nexus 3000 Series Hardware Installation Guide	Provides detailed information about site requirements, switch hardware details, and installation options.
Cisco Nexus 3000 Series Switch Software Configuration Guides (choose the guide for the NX-OS release installed on your switches)	Provides initial switch configuration information that you need before you can configure the switch for ONTAP operation.
Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide (choose the guide for the NX-OS release installed on your switches)	Provides information on how to downgrade the switch to ONTAP supported switch software, if necessary.
Cisco Nexus 3000 Series NX-OS Command Reference Master Index	Provides links to the various command references provided by Cisco.
Cisco Nexus 3000 MIBs Reference	Describes the Management Information Base (MIB) files for the Nexus 3000 switches.
Nexus 3000 Series NX-OS System Message Reference	Describes the system messages for Cisco Nexus 3000 series switches, those that are informational, and others that might help diagnose problems with links, internal hardware, or the system software.
Cisco Nexus 3000 Series NX-OS Release Notes (choose the notes for the NX-OS release installed on your switches)	Describes the features, bugs, and limitations for the Cisco Nexus 3000 Series.
Regulatory, Compliance, and Safety Information for the Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series	Provides international agency compliance, safety, and statutory information for the Nexus 3000 series switches.

ONTAP systems documentation

To set up an ONTAP system, you need the following documents for your version of the operating system from ONTAP 9.

Name	Description
Controller-specific *Installation and Setup Instructions*	Describes how to install NetApp hardware.
ONTAP documentation	Provides detailed information about all aspects of the ONTAP releases.

Name	Description
Hardware Universe	Provides NetApp hardware configuration and compatibility information.

Rail kit and cabinet documentation

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

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

Smart Call Home requirements

To use Smart Call Home, 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.

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.

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.

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

- 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

Hardware install workflow for Cisco Nexus 3232C switches

To install and configure the hardware for a 3232C storage switch, follow these steps:

1 Install the switch

Install the 3232C storage switch.

2 Install the switch in a NetApp cabinet

Install the 3232C storage switch and pass-through panel in a NetApp cabinet as required.

3 Review cabling and configuration considerations

Review the cabling and configuration considerations for the 3232C storage switch.

Install the 3232C storage switch

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

Before you begin

Make sure you have the following:

- 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.
- 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 and ONTAP documentation.

Steps

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

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

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

What's next?

After you've installed the 3232C storage switch, you can then install the switch in a NetApp cabinet.

Install a Cisco Nexus 3232C storage switch in a NetApp cabinet

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

Before you begin

Verify that you have the following:
* The initial preparation requirements, kit contents, and safety precautions in the Cisco Nexus 3000 Series Hardware Installation Guide.
* For each switch, the eight 10-32 or 12-24 screws and clip nuts to mount the brackets and slider rails to the front and rear cabinet posts.
* Cisco standard rail kit to install the switch in a NetApp cabinet.

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

Steps

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

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

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

   - One pass-through blanking panel
   - Four 10-32 x .75 screws
   - Four 10-32 clip nuts

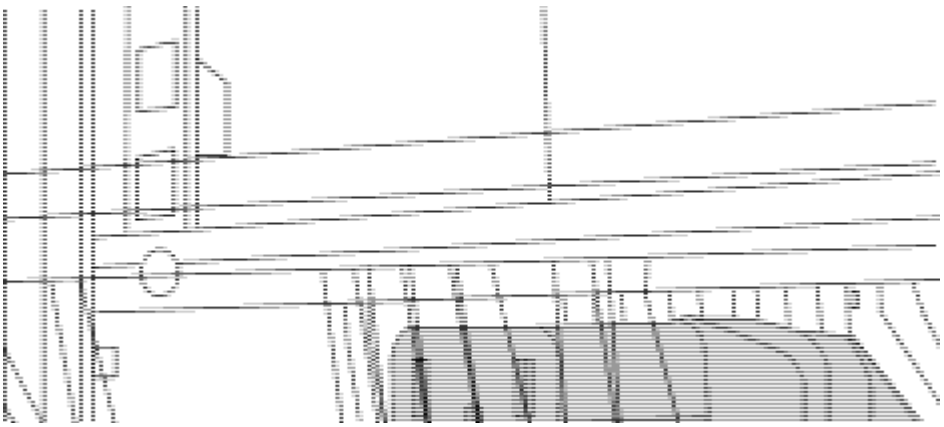
   a. Determine the vertical location of the switches and blanking panel in the cabinet.

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

   b. Install two clip nuts on each side in the appropriate square holes for front cabinet rails.

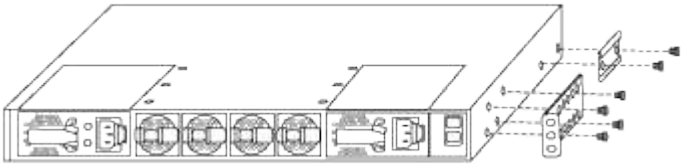
   c. Center the panel vertically to prevent intrusion into adjacent rack space, and then tighten the screws.

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

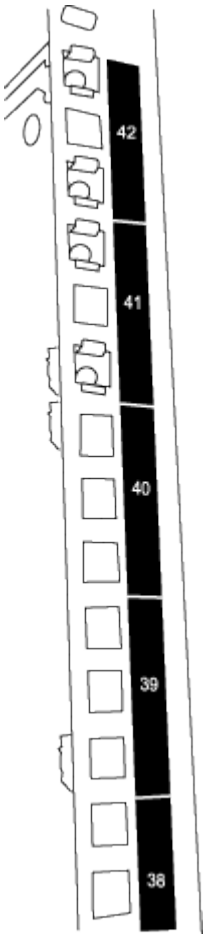


(1) Female connector of the jumper cord.

1. Install the rack-mount brackets on the Nexus 3232C storage switch chassis.
   a. Position a front rack-mount bracket on one side of the switch chassis so that the mounting ear is aligned with the chassis faceplate (on the PSU or fan side), and then use four M4 screws to attach the bracket to the chassis.

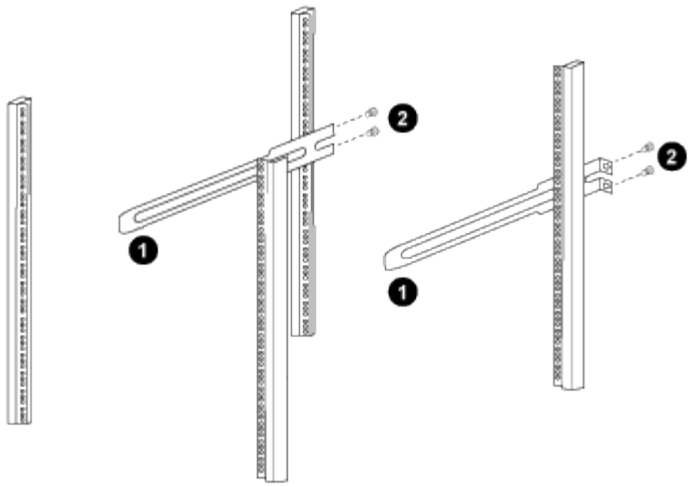


   b. Repeat step 2a with the other front rack-mount bracket on the other side of the switch.
   c. Install the rear rack-mount bracket on the switch chassis.
   d. Repeat step 2c with the other rear rack-mount bracket on the other side of the switch.
2. Install the clip nuts in the square hole locations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



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

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



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

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

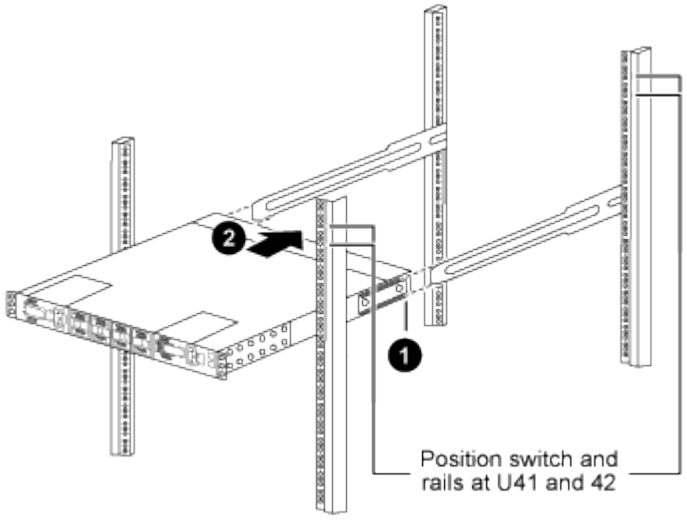
b. Repeat step 4a for the right side rear post.

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

4. Install the switch in the cabinet.

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

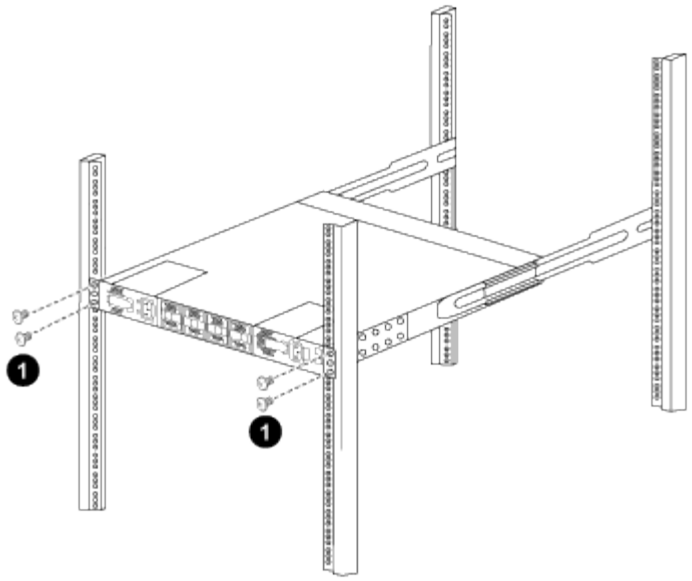
a. Position the back of the switch at RU41.



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

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

b. Attach the switch to the cabinet.



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

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

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

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

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

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

7. Connect the management port on each 3232C switch to either of the management switches (if ordered) or connect them directly to your management network.

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

Review cabling and configuration considerations

Before configuring your 3232C switches, review the cabling and configuration requirements.

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

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

```
(s1)(config)# interface Ethernet1/19
For 100GbE speed:
(s1)(config-if)# speed 100000
For 40GbE speed:
(s1)(config-if)# speed 40000
(s1)(config-if)# no negotiate auto
(s1)(config-if)# exit
(s1)(config)# exit
Save the changes:
(s1)# copy running-config startup-config
```

Related information

- Refer to Hardware Universe for more information on switch ports.
- See What additional information do I need to install my equipment that is not in HWU? for more information about switch installation requirements.

Configure software

Software install workflow for Cisco Nexus 3232C storage switches

To install and configure the software for a Cisco Nexus 3232C switch and install or upgrade the Reference Configuration File (RCF), follow these steps:

1. **Configure the switch**

Configure the 3232C storage switch.

2. **Prepare to install the NX-OS software and RCF**

The Cisco NX-OS software and reference configuration files (RCFs) must be installed on Cisco 3232C storage switches.

3. **Install or upgrade the NX-OS software**

Download and install or upgrade the NX-OS software on the Cisco 3232C storage switch.

4. **Install the RCF**

Install the RCF after setting up the Cisco 3232C storage switch for the first time.

5. **Upgrade the RCF**

Upgrade your existing RCF version as necessary.

6 Verify SSH configuration

Verify that SSH is enabled on the switches to use the Ethernet Switch Health Monitor (CSHM) and log collection features.

7 Reset the switch to factory defaults

Erase the 3232C storage switch settings.

Configure the 3232C storage switch

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

Before you begin

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

  See Required documentation for more information.
- Required controller documentation and ONTAP documentation.

  NetApp documentation
- Applicable licenses, network and configuration information, and cables.
- Applicable NetApp storage network and management network RCFs, downloaded from the NetApp Support Site at mysupport.netapp.com for the switches that you receive. All Cisco storage network and management network switches arrive with the standard Cisco factory-default configuration. These switches also have the current version of the NX-OS software, but do not have the RCFs loaded.

Steps

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

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

2. Cable the storage network and management network switches to the controllers using the completed cabling worksheets.
3. Power on the storage network and management network switches and controllers.
4. Perform an initial configuration of the storage network switches.

   Provide applicable responses to the following initial setup questions when you first boot the switch. Your

site's security policy defines the responses and services to enable.

Prompt	Response
Abort Auto Provisioning and continue with normal setup? (yes/no)	Respond with **yes**. The default is no.
Do you want to enforce secure password standard? (yes/no)	Respond with **yes**. The default is yes.
Enter the password for admin.	The default password is "admin"; you must create a new, strong password. A weak password can be rejected.
Would you like to enter the basic configuration dialog? (yes/no)	Respond with **yes** at the initial configuration of the switch.
Create another login account? (yes/no)	Your answer depends on your site's policies on alternate administrators. The default is **no**.
Configure read-only SNMP community string? (yes/no)	Respond with **no**. The default is no.
Configure read-write SNMP community string? (yes/no)	Respond with **no**. The default is no.
Enter the switch name.	The switch name is limited to 63 alphanumeric characters.
Continue with Out-of-band (mgmt0) management configuration? (yes/no)	Respond with **yes** (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip_address.
Configure the default-gateway? (yes/no)	Respond with **yes**. At the IPv4 address of the default-gateway: prompt, enter your default_gateway.
Configure advanced IP options? (yes/no)	Respond with **no**. The default is no.
Enable the telnet service? (yes/no)	Respond with **no**. The default is no.
Enabled SSH service? (yes/no)	Respond with **yes**. The default is yes. SSH is recommended when using Ethernet Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.

Prompt	Response
Enter the type of SSH key you want to generate (dsa/rsa/rsa1).	The default is **rsa**.
Enter the number of key bits (1024-2048).	Enter the number of key bits from 1024-2048.
Configure the NTP server? (yes/no)	Respond with **no**. The default is no.
Configure default interface layer (L3/L2):	Respond with **L2**. The default is L2.
Configure default switch port interface state (shut/noshut):	Respond with **noshut**. The default is noshut.
Configure CoPP system profile (strict/moderate/lenient/dense):	Respond with **strict**. The default is strict.
Would you like to edit the configuration? (yes/no)	You should see the new configuration at this point. Review and make any necessary changes to the configuration you just entered. Respond with **no** at the prompt if you are satisfied with the configuration. Respond with **yes** if you want to edit your configuration settings.
Use this configuration and save it? (yes/no)	Respond with **yes** to save the configuration. This automatically updates the kickstart and system images. If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch.

5. Verify the configuration choices you made in the display that appears at the end of the setup, and make sure that you save the configuration.
6. Check the version on the 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?

After you've configured your switches, you can prepare to install the NX-OS and RCF.

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

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

About the examples

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

- The names of the two Cisco switches are s1 and s2.
- The node names are cluster1-01 and cluster1-02.

See the Hardware Universe to verify the correct network ports on your platforms. See What additional information do I need to install my equipment that is not in HWU? for more information about switch installation requirements.

About this task

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

Steps

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

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

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

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

   `set -privilege advanced`

   The advanced prompt (`*>`) appears.

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

   `network device-discovery show -protocol cdp`

Show example

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
            e5a    s1                        Eth1/2            N3K-
C3232C
            e3b    s2                        Eth1/2            N3K-
C3232C
cluster1-01/cdp
            e5a    s1                        Eth1/1            N3K-
C3232C
            e3b    s2                        Eth1/1            N3K-
C3232C
.
.
```

4. Check the administrative or operational status of each node storage port and storage shelf port.
   a. Display the node storage port attributes:

      ```
      storage port show
      ```

      Show example

      ```
      cluster1::*> storage port show
      Speed                       VLAN
      Node           Port Type  Mode    (Gb/s) State    Status      ID
      -------------- ---- ----- ------- ------ -------- --------- ----
      cluster1-01
                     e5a  ENET  storage    100 enabled  online      -
                     e3b  ENET  storage    100 enabled  online      -
      cluster1-02

                     e5a  ENET  storage    100 enabled  online      -
                     e3b  ENET  storage    100 enabled  online      -
      .
      .
      ```

b. Display the storage shelf port attributes:

```
storage shelf port show
```

Show example

```
cluster1::*> storage shelf port show
Shelf ID Module State        Internal?
-------- -- ------ ---------- ---------
1.4
         0 A      connected    false
         1 A      connected    false
         2 B      connected    false
         3 B      connected    false
.
.
```

c. Verify that switch health monitoring (CSHM) is enabled for the switches so that they are monitored:

```
system switch ethernet show
```

Show example

```
cluster1::> system switch ethernet show
  Switch              Type               Address          Model
  ------------------ ------------------ ----------------
---------------
  s1                  storage-network    1.0.0.0          N3K-
C3232C
     Serial Number: FFFYYYYYYY1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2                  storage-network    1.1.0.0           N3K-
C3232C
     Serial Number: FEEYYYYYYY2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

What's next?

After you've prepared to install the NX-OS software and RCF, you can install the NX-OS software.

Install or upgrade the NX-OS software

You can use this procedure to install the NX-OS software on the Nexus 3232C storage switch.

Before you begin

Verify that you have the following:

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

Install or upgrade the software

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

Complete the procedure in Prepare to install NX-OS and RCF, and then follow the steps below.

Steps

1. Connect the 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:

   ```
   s2# 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. If you are setting up your switch for the first time, skip to step 5. If you are upgrading your switch, proceed to the next step.
4. Check the administrative or operational status of each node storage port and storage shelf port.
   a. Display the node storage port attributes:

      ```
      storage port show
      ```

      Show example

      ```
      cluster1::*> storage port show
      Speed                      VLAN
      Node           Port Type   Mode    (Gb/s) State    Status      ID
      -------------- ---- ------ ------- ------ -------- --------- ----
      cluster1-01
                     e5a  ENET   storage    100 enabled  online      -
                     e3b  ENET   storage    100 enabled  online      -
      cluster1-02

                     e5a  ENET   storage    100 enabled  online      -
                     e3b  ENET   storage    100 enabled  online      -
      .
      .
      ```

   b. Display the storage shelf port attributes:

`storage shelf port show`

Show example

```
cluster1::*> storage shelf port show
Shelf ID Module State        Internal?
----- -- ------ ------------ ---------
1.4
       0 A      connected    false
       1 A      connected    false
       2 B      connected    false
       3 B      connected    false
.
.
```

c. Verify that switch health monitoring (CSHM) is enabled for the switches so that they are monitored:

`system switch ethernet show`

Show example

```
cluster1::> system switch ethernet show
  Switch             Type               Address          Model
  ----------------- ------------------ ----------------
---------------
  s1                 storage-network    1.0.0.0          N3K-
C3232C
     Serial Number: FFFYYYYYYY1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2                 storage-network    1.1.0.0           N3K-
C3232C
     Serial Number: FEEYYYYYYY2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

5. Log in to the switch using SSH or by using a serial console.
6. Copy the NX-OS software and EPLD images to the Nexus 3232C switch.

Show example

```
s2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


s2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.4.img  /bootflash/n9000-
epld.9.3.4.img
/code/n9000-epld.9.3.4.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

```
show version
```

Show example

```
s2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.37
  NXOS: version 9.3(3)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.3.bin
  NXOS compile time:  12/22/2019 2:00:00 [12/22/2019 14:00:37]

Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGD

  Device name: s2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 36 second(s)

Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
  Reason: Reset Requested by CLI command reload
```

```
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

8. Install the NX-OS image.

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

Show example

```
s2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

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

Compatibility check is done:
Module  bootable          Impact              Install-type  Reason
------- ----------------- ------------------- -------------
----------
     1     Yes            Disruptive          Reset         Default
upgrade is not hitless

Images will be upgraded according to following table:
Module       Image       Running-Version(pri:alt)
New-Version          Upg-Required
------------ ----------- ---------------------------------------
-------------------- ------------
     1       nxos        9.3(3)
9.3(4)               yes
     1       bios        v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(01/28/2020)   no


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

Install is in progress, please wait.
```

```
Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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


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

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

   ```
   show version
   ```

Show example

```
s2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.37
  NXOS: version 9.3(4)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 06:28:31]

Hardware
 cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGS

  Device name: rtpnpi-mcc01-8200-ms-A1
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)

Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
  Reason: Reset due to upgrade
```

```
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

10. Upgrade the EPLD image and reboot the switch.

Show example

```
s2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                            0x12
IO   FPGA                            0x11

s2# install epld bootflash:n9000-epld.9.3.4.img module 1
Compatibility check:
Module        Type         Upgradable    Impact      Reason
------  -----------------  ----------    ----------
-----------------
     1         SUP         Yes           Disruptive  Module
Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------  ----  -----------------  ---------------   -----------
------------
     1   SUP   MI FPGA                0x12         0x12         No
     1   SUP   IO FPGA                0x11         0x12         Yes
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64
sectors)
Module 1 EPLD upgrade is successful.
Module        Type  Upgrade-Result
------  ------------------  --------------
     1         SUP         Success

Module 1 EPLD upgrade is successful.
```

11. If you are upgrading to NX-OS version 9.3(11), you must upgrade the EPLD `golden` image and reboot the switch once again. Otherwise, skip to step 12.

See EPLD Upgrade Release Notes, Release 9.3(11) for further details.

Show example

```
s2# install epld bootflash:n9000-epld.9.3.11.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module        Type         Upgradable     Impact      Reason
------  -----------------  -------------  ----------
-----------------
     1        SUP          Yes            Disruptive  Module
Upgradable

Retrieving EPLD versions.... Please wait.
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

 Starting Module 1 EPLD Upgrade

Module 1 : MI FPGA [Programming] : 100.00% (     64 of      64 sect)
Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sect)
Module 1 EPLD upgrade is successful.
Module        Type          Upgrade-Result
------  ------------------  --------------
     1         SUP          Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

12. After the switch reboot, log in to verify that the new version of EPLD loaded successfully.

Show example

```
s2# show version module 1 epld

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

13. If you are setting up your switch for the first time, skip to step 15. If you are upgrading your switch, proceed to the next step.
14. Verify the health status of each node storage port and storage shelf port.
    a. Display the node storage port attributes:

    ```
    storage port show
    ```

    Show example

    ```
    cluster1::*> storage port show
    Speed                      VLAN
    Node           Port Type   Mode    (Gb/s) State    Status      ID
    -------------- ---- ------ ------- ------ -------- --------- ----
    cluster1-01
                   e5a  ENET   storage    100 enabled  online      -
                   e3b  ENET   storage    100 enabled  online      -
    cluster1-02

                   e5a  ENET   storage    100 enabled  online      -
                   e3b  ENET   storage    100 enabled  online      -
    ```

    b. Display the storage shelf port attributes:

    ```
    storage shelf port show
    ```

    Show example

    ```
    cluster1::*> storage shelf port show
    Shelf ID Module State         Internal?
    ----- -- ------ ------------ ---------
    1.4
           0 A      connected    false
           1 A      connected    false
           2 B      connected    false
           3 B      connected    false
    .
    .
    ```

    c. Verify that switch health monitoring (CSHM) is enabled for the switches so that they are monitored:

    ```
    system switch ethernet show
    ```

Show example

```
cluster1::> system switch ethernet show
  Switch            Type               Address          Model
  ----------------- ------------------ ---------------
---------------
  s1                storage-network    1.0.0.0          N3K-
C3232C
     Serial Number: FFFYYYYYYY1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2                storage-network    1.1.0.0           N3K-
C3232C
     Serial Number: FEEYYYYYYY2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP  false
```

15. Repeat steps 5 to 13 to install the NX-OS software on switch s1.

What's next?

After you've installed the NX-OS software, you can install or upgrade the Reference Configuration File (RCF).

Install the Reference Configuration File (RCF)

You install the Reference Configuration File (RCF) after setting up the Nexus 3232C switches for the first time.

Before you begin

Verify the following installations and connections:

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs or similar issues).
- The current RCF.
- A console connection to the switch, this is required when installing the RCF.

About this task

The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 Series Switches

commands; ONTAP commands are used unless otherwise indicated.

Complete the procedure in Prepare to install NX-OS and RCF, and then follow the steps below.

Step 1: Install the RCF on the switches

1. Login to switch s2 using SSH or by using a serial console.
2. Copy the RCF to the bootflash of switch s2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Command Reference.

   Show example

   This example shows TFTP being used to copy an RCF to the bootflash on switch s2:

   ```
   s2# copy tftp: bootflash: vrf management
   Enter source filename: NX3232C-RCF-v1.13-1-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 3000 Series NX-OS Command Reference.

   Show example

   This example shows the RCF file `NX9336C-FX2-RCF-v1.13-1-Storage.txt` being installed on switch s2:

   ```
   s2# copy NX9336C-FX2-RCF-v1.13-1-Storage.txt running-config echo-
   commands
   ```

   Make sure to read thoroughly the **Installation notes**, **Important Notes**, and **banner** sections of your RCF. You must read and follow these instructions to verify the proper configuration and operation of the switch.

4. Examine the banner output from the `show banner motd` command. You must read and follow the instructions under **Important Notes** to make sure the proper configuration and operation of the switch.
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.
7. After you verify that the RCF versions and switch settings are correct, copy the `running-config` file to the `startup-config` file.

   ```
   s2# copy running-config startup-config [] 100% Copy complete
   ```

8. Reboot switch s2:

   ```
   s2# reload

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

9. Repeat Steps 1 to 8 on switch s1.
10. Connect the node storage ports and storage shelf ports of all nodes in the ONTAP cluster to switches s1 and s2.

Step 2: Verify the switch connections

1. Verify that the switch ports are **up**.

   ```
   show interface brief
   ```

2. Verify that the node storage ports and storage shelf ports are in their correct VLANs using the following commands:

   ```
   show vlan brief

   show interface trunk
   ```

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 set up and configuration including assigning a node management IP address, initializing the cluster, creating a local tier, configuring protocols, and provisioning initial storage.

Refer to Configure ONTAP on a new cluster with System Manager for setup instructions.

What's next?

After you've installed the RCF, you can verify the SSH configuration.

Upgrade your Reference Configuration File (RCF)

You upgrade your RCF version when you have an existing version of the RCF file installed on your operational switches.

Before you begin

Make sure you have the following:

- A current backup of the switch configuration.
- A fully functioning cluster (no errors in the logs or similar issues).
- The current RCF.
- If you are updating your RCF version, you need a boot configuration in the RCF that reflects the desired boot images.

  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 included in future reboots.

> 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 or have preserved basic configuration information before erasing the switch settings.

Step 1: Prepare for the upgrade

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

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

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

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

   ```
   set -privilege advanced
   ```

   The advanced prompt (*>) appears.

3. Display the ports on each node that are connected to the 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
            e5a    s1                      Ethernet1/7     N3K-
C3232C
            e3b    s2                      Ethernet1/7     N3K-
C3232C
cluster1-02/cdp
            e5a    s1                      Ethernet1/8     N3K-
C3232C
            e3b    s2                      Ethernet1/8     N3K-
C3232C
.
.
```

4. Check the administrative or operational status of each node storage port and storage shelf port.
   a. Verify that all the node storage ports are up with a healthy status:

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

Show example

```
cluster1::*> storage port show -port-type ENET


                                  Speed
Node               Port Type  Mode    (Gb/s) State    Status
------------------ ---- ----- ------- ------ -------- -----------
cluster1-01
                   e5a ENET  -         100   enabled  online
                   e3b ENET  -         100   enabled  online
cluster1-02
                   e5a ENET  -         100   enabled  online
                   e3b ENET  -         100   enabled  online
.
.
```

b. Verify that all the storage shelf ports are up with a healthy status:

```
storage shelf port show
```

Show example

```
cluster1::> storage shelf port show

Shelf ID Module State        Internal?
----- -- ------ ------------ ---------
1.4
       0 A      connected    false
       1 A      connected    false
       2 B      connected    false
       3 B      connected    false
.
.
```

c. Verify that the switches are being monitored.

```
system switch ethernet show
```

Show example

```
cluster1::*> system switch ethernet show
  Switch            Type               Address          Model
  ----------------- ------------------ ---------------
---------------
  s1                storage-network    1.2.3.4          N3K-
C3232C
     Serial Number: FFFXXXXXXX1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2                storage-network    2.3.4.5          N3K-
C3232C
     Serial Number: FEEXXXXXXX2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

Step 2: Upgrade the RCF

1. Log in to switch s2 using SSH or by using a serial console.
2. Shut down the ports connected to all of the ports of the nodes.

```
s2> enable
s2# configure
s2(config)# interface e1/1-32
s2(config-if-range)# shutdown
s2(config-if-range)# exit
s2(config)# exit
```

Make sure to shutdown **all** connected ports to avoid any network connection issues. See the Knowledge Base article Node out of quorum when migrating cluster LIF during switch OS upgrade for further details.

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

```
show running-config
```

a. Record any custom additions between the current `running-config` and the RCF file in use (such as an SNMP configuration for your organization).

b. For NX-OS 10.2 and later, use the `show diff running-config` command to compare with the saved RCF file in the bootflash. Otherwise, use a third-party diff or compare tool.

4. Save basic configuration details to the `write_erase.cfg` file on the bootflash.

Make sure to configure the following:

- Username and password
- Management IP address
- Default gateway
- Switch name

```
s2# show run | section "switchname" > bootflash:write_erase.cfg

s2# show run | section "hostname" >> bootflash:write_erase.cfg

s2# show run | i "username admin password" >> bootflash:write_erase.cfg

s2# show run | section "vrf context management" >> bootflash:write_erase.cfg

s2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

See the Knowledge Base article How to clear configuration on a Cisco interconnect switch while retaining remote connectivity for further details.

5. Verify that the `write_erase.cfg` file is populated as expected:

```
show file bootflash:write_erase.cfg
```

6. Issue the `write erase` command to erase the current saved configuration:

```
s2# write erase

Warning: This command will erase the startup-configuration.

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

7. Copy the previously saved basic configuration into the startup configuration.

```
s2# copy bootflash:write_erase.cfg startup-config
```

8. Reboot the switch:

```
s2# reload

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

9. After the management IP address is reachable again, log in to the switch through SSH.

   You might need to update host file entries related to the SSH keys.

10. Copy the RCF to the bootflash of switch s2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP.

    For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series NX-OS Documentation.

    Show example

    This example shows TFTP being used to copy an RCF to the bootflash on switch s2:

    ```
    s2# copy tftp: bootflash: vrf management
    Enter source filename: NX3232C-RCF-v1.13-1-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)...
    ```

11. Apply the RCF previously downloaded to the bootflash.

    For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 3000 Series documentation.

    This example shows the RCF file `NX3232C-RCF-v1.13-1-Storage.txt` being installed on switch s2:

    ```
    s2# copy NX3232C-RCF-v1.13-1-Storage.txt running-config echo-commands
    ```

    Make sure to thoroughly read the **Installation notes**, **Important Notes**, and **banner** sections of your RCF. You must read and follow these instructions to ensure the proper configuration and operation of the switch.

12. Verify that the RCF file is the correct newer version:

    ```
    show running-config
    ```

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

    - The RCF banner
    - The node and port settings
    - Customizations

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

13. Reapply any previous customizations to the switch configuration.
14. After you verify the RCF versions, custom additions, 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 documentation.

    ```
    s2# copy running-config startup-config

    [] 100% Copy complete
    ```

15. Reboot switch s2. You can ignore the “cluster switch health monitor” alerts and “cluster ports down” events reported on the nodes while the switch reboots.

    ```
    s2# reload

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

16. Check the administrative or operational status of each node storage port and storage shelf port.
    a. Verify that all the storage ports are up with a healthy status:

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

    Show example

    ```
    cluster1::*> storage port show -port-type ENET


                                         Speed
    Node               Port Type  Mode    (Gb/s) State    Status
    ------------------ ---- ----- ------- ------ -------- -----------
    cluster1-01
                       e5a  ENET  -          100 enabled  online
                       e3b  ENET  -          100 enabled  online
    cluster1-02
                       e5a  ENET  -          100 enabled  online
                       e3b  ENET  -          100 enabled  online
    .
    .
    ```

    b. Verify that all the storage shelf ports are up with a healthy status:

    ```
    storage shelf port show
    ```

Show example

```
cluster1::> storage shelf port show

Shelf ID Module State        Internal?
----- -- ------ ------------ ---------
1.4
       0 A      connected    false
       1 A      connected    false
       2 B      connected    false
       3 B      connected    false
.
.
```

c. Verify that the switches are being monitored:

```
system switch ethernet show
```

Show example

```
cluster1::*> system switch ethernet show
  Switch           Type               Address          Model
  ---------------- ------------------ ----------------
---------------
  s1               storage-network    1.2.3.4          N3K-C3232C
     Serial Number: FFFXXXXXXX1
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
  s2               storage-network    2.3.4.5          N3K-C3232C
     Serial Number: FEEXXXXXXX2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    10.3(4a)
    Version Source: CDP/ISDP
```

17. Repeat steps 1 to 16 on switch s1.

Step 3: Verify the storage network

Complete the following steps on each storage switch to verify that the storage network is functioning properly after the RCF upgrade.

1. Verify that the switch ports are **up**.

```
show interface brief
```

2. Verify that the expected node storage ports are still connected:

```
show cdp neighbors
```

3. Verify that the expected storage shelf ports are still connected:

```
show lldp neighbors
```

4. Verify that the node storage ports and storage shelf ports are in their correct VLANs using the following commands:

```
show vlan brief
```

```
show interface trunk
```

What's next?

After you've upgraded your RCF, you can verify the SSH configuration.

Verify your SSH configuration

If you are using the Ethernet Switch Health Monitor (CSHM) and log collection features, verify that SSH and SSH keys are enabled on the switches.

Steps

1. Verify that SSH is enabled:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Verify that the SSH keys are enabled:

```
show ssh key
```

Show example

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

When enabling FIPS, you must change the bitcount to 256 on the switch using the command `ssh key ecdsa 256 force`. See Configure network security using FIPS for more details.

What's next?

After you've verified your SSH configuration, you can configure switch health monitoring.

Reset the 3232C storage switch to factory defaults

To reset the 3232C storage switch to factory defaults, you must erase the 3232C storage switch settings.

About this task

- You must be connected to the switch using the serial console.
- This task resets the configuration of the management network.

Steps

1. Erase the existing configuration:

   `write erase`

   ```
   (s2)# write erase

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

2. Reload the switch software:

   `reload`

   ```
   (s2)# reload

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

   The system reboots and enters the configuration wizard. During the boot, if you receive the prompt “Abort Auto Provisioning and continue with normal setup? (yes/no)[n]”, you should respond **yes** to proceed.

What’s next

After resetting the switch, you can reconfigure it according to your requirements.

Replace a Cisco Nexus 3232C storage switch

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

Review requirements

The existing network configuration must have the following characteristics:

- The Cisco Ethernet Switches page has the latest RCF and NX-OS versions on your switches.
- Management connectivity must exist on both switches.

Make sure that all troubleshooting steps have been completed to confirm that your switch needs replacing.

The replacement Cisco Nexus 3232C switch must have the following characteristics:

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

Replace the switch

This procedure replaces the second Nexus 3232C storage switch s2 with the new 3232C switch ns2. The two nodes are cluster1-01 and cluster1-02.

Step 1: Confirm the switch to be replaced is s2

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

   x is the duration of the maintenance window in hours.

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

2. Check on the health status of the storage node ports to make sure that there is connection to storage switch s1:

   `storage port show -port-type ENET`

Show example

```
storage::*> storage port show -port-type ENET
                                     Speed                       VLAN
Node               Port Type  Mode    (Gb/s) State    Status      ID
------------------ ---- ----- ------- ------ -------- --------- ----
cluster1-01
                   e5a  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
cluster1-02
                   e5a  ENET  storage    100 enabled  online      30
                   e3b  ENET  storage      0 enabled  offline     30
                   e7a  ENET  storage      0 enabled  offline     30
                   e7b  ENET  storage      0 enabled  offline     30
```

3. Verify that storage switch s1 is available:

   `network device-discovery show`

Show example

```
storage::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
----------------
cluster1-01/cdp
            e5a    s1                        Ethernet1/1
NX3232C
            e4a    cluster1-02                     e4a
AFF-A700
            e4e    cluster1-02                     e4e
AFF-A700
cluster1-01/lldp
            e5a    s1                        Ethernet1/1       -
            e4a    cluster1-02                     e4a
-
            e4e    cluster1-02                     e4e
-
cluster1-02/cdp
            e3a    s1                        Ethernet1/2
NX3232C
            e4a    cluster1-01                     e4a
AFF-A700
            e4e    cluster1-01                     e4e
AFF-A700
cluster1-02/lldp
            e3a    s1                        Ethernet1/2       -
            e4a    cluster1-01                     e4a
-
            e4e    cluster1-01                     e4e
-
.
.
```

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

   `show lldp neighbors`

Show example

```
s1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID               Local Intf      Hold-time  Capability  Port
ID
cluster1-01             Eth1/1          121        S           e5a
cluster1-02             Eth1/2          121        S           e5a
SHFGD2008000011         Eth1/5          121        S           e0a
SHFGD2008000011         Eth1/6          120        S           e0a
SHFGD2008000022         Eth1/7          120        S           e0a
SHFGD2008000022         Eth1/8          120        S           e0a
```

Step 2: Configure cabling

1. Verify the shelf ports in the storage system:

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

   Show example

```
storage::*> storage shelf port show -fields remote-device,remote-
port

shelf  id  remote-port  remote-device
-----  --  -----------  -------------
3.20   0   Ethernet1/5  s1
3.20   1   -            -
3.20   2   Ethernet1/6  s1
3.20   3   -            -
3.30   0   Ethernet1/7  s1
3.20   1   -            -
3.30   2   Ethernet1/8  s1
3.20   3   -            -
```

2. Remove all cables attached to storage switch s2.
3. Reconnect all cables to the replacement switch ns2.

Step 3: Verify all device configurations on switch ns2

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

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

Show example

```
storage::*> storage port show -port-type ENET
                                     Speed
VLAN
Node                Port Type  Mode    (Gb/s) State    Status
ID
------------------ ---- ----- ------- ------ -------- ------------
---
cluster1-01
                    e5a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30
cluster1-02
                    e5a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30

.
.
```

2. Verify that both switches are available:

```
network device-discovery show
```

Show example

```
storage::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e5a    s1                        Ethernet1/1
NX3232C
            e4a    cluster1-02               e4a               AFF-
A700
            e4e    cluster1-02               e4e               AFF-
A700
            e7b    ns2                       Ethernet1/1
NX3232C
cluster1-01/lldp
            e5a    s1                        Ethernet1/1       -
            e4a    cluster1-02               e4a               -
            e4e    cluster1-02               e4e               -
            e7b    ns2                       Ethernet1/1       -
cluster1-02/cdp
            e5a    s1                        Ethernet1/2
NX3232C
            e4a    cluster1-01               e4a               AFF-
A700
            e4e    cluster1-01               e4e               AFF-
A700
            e7b    ns2                       Ethernet1/2
NX3232C
cluster1-02/lldp
            e5a    s1                        Ethernet1/2       -
            e4a    cluster1-01               e4a               -
            e4e    cluster1-01               e4e               -
            e7b    ns2                       Ethernet1/2       -
.
.
```

3. Verify the shelf ports in the storage system:

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

Show example

```
storage::*> storage shelf port show -fields remote-device,remote-
port
shelf id remote-port remote-device
----- -- ----------- -------------
3.20  0  Ethernet1/5 s1
3.20  1  Ethernet1/5 ns2
3.20  2  Ethernet1/6 s1
3.20  3  Ethernet1/6 ns2
3.30  0  Ethernet1/7 s1
3.20  1  Ethernet1/7 ns2
3.30  2  Ethernet1/8 s1
3.20  3  Ethernet1/8 ns2
.
.
```

4. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

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

What's next?

After you've replaced your switch, you can configure switch health monitoring.

Upgrade a Cisco Nexus 3232C storage switch

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

Review requirements

Before you begin

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

- The switch is fully functioning (there should be no errors in the logs or similar issues).
- You have checked or set your desired boot variables in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.

  If you need to change the boot variables to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.

- You have referred to the appropriate software and upgrade guides available on the Cisco Nexus 3000 Series Switches page for complete documentation on the Cisco storage upgrade and downgrade procedures.
- The number of 10 GbE and 40/100 GbE ports are defined in the reference configuration files (RCFs) available on the Cisco® Ethernet Switches page.

Replace the switch

About the examples

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

- The names of the two storage switches are s1 and s2.
- The nodes are cluster1-01 and cluster1-02.

The examples in this procedure use two nodes; cluster1-01 with two storage ports and cluster1-02 with two storage ports. See the Hardware Universe to verify the correct storage ports on your platforms. See What additional information do I need to install my equipment that is not in HWU? for more information about switch installation requirements.

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

Step 1: Check the health status of switches and ports

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

   x is the duration of the maintenance window in hours.

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

2. Check that the storage switches are available:

   ```
   system switch ethernet show
   ```

Show example

```
storage::*> system switch ethernet show
Switch                    Type               Address          Model
------------------------- ------------------ ----------------
---------------
s1
                          storage-network    172.17.227.5     NX3232C
     Serial Number: FOC221206C2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(3)
    Version Source: CDP

s2
                          storage-network    172.17.227.6     NX3232C
     Serial Number: FOC220443LZ
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(3)
    Version Source: CDP

2 entries were displayed.
storage::*>
```

3. Verify that the node ports are healthy and operational:

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

Show example

```
storage::*> storage port show -port-type ENET
                                      Speed
VLAN
Node                Port Type  Mode    (Gb/s) State    Status
ID
------------------- ---- ----- ------- ------ -------- -----------
----
cluster1-01
                    e5a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30
cluster1-02
                    e5a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30
.
.
```

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

   `system health alert show -instance`

   Show example

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

Step 2: Copy the RCF to Cisco switch s2

1. Copy the RCF on switch s2 to the switch bootflash using one of the following transfer protocols: FTP, HTTP, TFTP, SFTP, or SCP.

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

Show example

The following example shows HTTP being used to copy an RCF to the bootflash on switch s2:

```
s2# copy http://172.16.10.1//cfg/Nexus_3232C_RCF_v1.6-Storage.txt
bootflash: vrf management
% Total    % Received % Xferd  Average  Speed   Time    Time
Time                           Current
                                Dload    Upload  Total   Spent
Left                           Speed
  100        3254       100    3254     0       0       8175     0
--:--:-- --:--:-- --:--:-   8301
Copy complete, now saving to disk (please wait)...
Copy complete.
s2#
```

2. Apply the RCF previously downloaded to the bootflash:

   `copy bootflash:`

   Show example

   The following example shows the RCF file `Nexus_3232C_RCF_v1.6-Storage.txt` being installed on switch s2:

   ```
   s2# copy Nexus_3232C_RCF_v1.6-Storage.txt running-config echo-
   commands
   ```

3. Verify that the RCF file is the correct newer version:

   `show running-config`

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

   - The RCF banner
   - The node and port settings
   - Customizations

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

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

Show example

```
s2# show banner motd

*****************************************************************
*************
* NetApp Reference Configuration File (RCF)
*
* Switch   : Cisco Nexus 3232C
* Filename : Nexus_3232C_RCF_v1.6-Storage.txt
* Date     : Oct-20-2020
* Version  : v1.6
*
* Port Usage : Storage configuration
* Ports  1-32: Controller and Shelf Storage Ports
* Ports 33-34: Disabled
*
* IMPORTANT NOTES*
* - This RCF utilizes QoS and requires TCAM re-configuration,
requiring RCF
*   to be loaded twice with the Storage Switch rebooted in
between.
*
* - Perform the following 4 steps to ensure proper RCF
installation:
*
*   (1) Apply RCF first time, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class
IPv4 ingress...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*       - Syntax error while parsing...
*
*   (4) Save running-configuration again
*****************************************************************
*************
s2#
```

When applying the RCF for the first time, the **ERROR: Failed to write VSH commands** message is expected and can be ignored.

4. After you verify that the software versions and switch settings are correct, copy the `running-config` file to the `startup-config` file on switch s2.

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

   Show example

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

   ```
   s2# copy running-config startup-config
   [########################################] 100% Copy complete.
   ```

Step 3: Copy the NX-OS image to Cisco switch s2 and reboot

1. Copy the NX-OS image to switch s2.

Show example

```
s2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

s2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.4.img  /bootflash/n9000-
epld.9.3.4.img
/code/n9000-epld.9.3.4.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

2. Install the system image so that the new version will be loaded the next time switch S2 is rebooted.

   The switch will be reboot in 10 seconds with the new image as shown in the following output:

Show example

```
s2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

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


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


Images will be upgraded according to following table:
Module       Image                  Running-Version(pri:alt)
New-Version  Upg-Required
------  ----------  ----------------------------------------
--------------------  ------------
     1        nxos                                      9.3(3)
9.3(4)           yes
     1        bios     v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)            no


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

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

Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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


Finishing the upgrade, switch will reboot in 10 seconds.
s2#
```

3. Save the configuration.

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

   You are prompted to reboot the system.

   Show example

```
s2# copy running-config startup-config
[] 100% Copy complete.
s2# reload
This command will reboot the system. (y/n)?  [n] y
```

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

Show example

```
s2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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


Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: S2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)

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

```
  Reason: Reset due to upgrade
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

s2#
```

Step 4: Recheck the health status of switches and ports

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

   ```
   system switch ethernet show
   ```

Show example

```
storage::*> system switch ethernet show
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
s1
                            storage-network    172.17.227.5
NX3232C
     Serial Number: FOC221206C2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(4)
    Version Source: CDP

s2
                            storage-network    172.17.227.6
NX3232C
     Serial Number: FOC220443LZ
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(4)
    Version Source: CDP
```

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

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

Show example

```
storage::*> storage port show -port-type ENET
                                      Speed
VLAN
Node                Port Type  Mode    (Gb/s) State    Status
ID
------------------ ---- ----- ------- ------ -------- -----------
----
cluster1-01
                    e5a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30
cluster1-02
                    e5a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30
```

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

   `system health alert show -instance`

   Show example

   ```
   storage::*> system health alert show -instance
   There are no entries matching your query.
   ```

4. Repeat the procedure to upgrade the NX-OS software and RCF on switch s1.
5. If you suppressed automatic case creation, re-enable it by invoking an AutoSupport message:

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

What's next?

After you've upgraded your switch, you can configure switch health monitoring.

NVIDIA SN2100

Get started

Installation and setup workflow for NVIDIA SN2100 switches

The NVIDIA SN2100 is an Ethernet switch that allows you to switch data between controllers and disk shelves.

Follow these workflow steps to install and setup your to SN2100 switches.

1. **Review the configuration requirements**

Review the configuration requirements for the SN2100 storage switch.

2. **Review the components and part numbers**

Review the components and part numbers for the SN2100 storage switch.

3. **Review the required documentation**

Review specific switch and controller documentation to set up your SN2100 switches and the ONTAP cluster.

4. **Install the hardware**

Install the switch hardware.

5. **Configure the software**

Configure the switch software.

Configuration requirements for NVIDIA SN2100 switches

For NVIDIA SN2100 switch installation and maintenance, be sure to review all requirements.

Installation requirements

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

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

For cabling guidelines, see Cabling and configuration considerations.

ONTAP and Linux support

The NVIDIA SN2100 switch is a 10/25/40/100 Gb Ethernet switch running Cumulus Linux. The switch supports the following:

- ONTAP 9.10.1P3. The SN2100 switch serves Cluster and Storage applications in ONTAP 9.10.1P3 over different switch-pairs. From ONTAP 9.10.1P3, you can use NVIDIA SN2100 switches to combine storage and cluster functionality into a shared switch configuration.
- Cumulus Linux (CL) OS version 4.4.3. For current compatibility information, see the NVIDIA Ethernet Switches information page.
- You can install Cumulus Linux when the switch is running Cumulus Linux or ONIE.

What's next

After you've reviewed the configuration requirements, you can confirm your components and part numbers.

Components and part numbers for NVIDIA SN2100 switches

For NVIDIA SN2100 switch installation and maintenance, be sure to review the list of components and part numbers for the cabinet and rail kit.

Cabinet details

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

Rail kit details

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

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

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

What's next

After you've confirmed your components and part numbers, you can review the required documentation.

Documentation requirements for NVIDIA SN2100 switches

For NVIDIA SN2100 switch installation and maintenance, be sure to review all the recommended documentation.

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

Title	Description
Setup and configure your NVIDIA SN2100 switches	Describes how to setup and configure your NVIDIA SN2100 switches, including installing Cumulus Linux and applicable RCFs.
Migrate from a Cisco storage switch to a NVIDIA SN2100 storage switch	Describes how to migrate from environments that use Cisco storage switches to environments that use NVIDIA SN2100 storage switches.
Migrate to a two-node switched cluster with NVIDIA SN2100 cluster switches	Describes how to migrate to a two-node switched environment using NVIDIA SN2100 cluster switches.
Replace a NVIDIA SN2100 storage switch	Describes the procedure to replace a defective NVIDIA SN2100 storage switch and download Cumulus Linux and reference configuration file.

Install hardware

Hardware install workflow for NVIDIA SN2100 storage switches

To install and configure the hardware for a SN2100 storage switch, follow these steps:

1. **Install the hardware**

Install the switch hardware.

2. **Review cabling and configuration considerations**

Review requirements for optical connections, the QSA adapter, and the switchport speed.

3. **Cable the NS224 shelves**

Follow the cabling procedures if you have a system in which the NS224 drive shelves need to be cabled as switch-attached storage (not direct-attached storage).

Install the hardware for the NVIDIA SN2100 switch

To install the SN2100 hardware, refer to NVIDIA's documentation.

Steps

1. Review the configuration requirements.

2. Follow the instructions in NVIDIA Switch Installation Guide.

What's next?

After you've installed your hardware, you can review cabling and configuration requirements.

Review cabling and configuration considerations

Before configuring your NVIDIA SN2100 switch, review the following considerations.

NVIDIA port details

Switch ports	Ports usage
swp1s0-3	4x10GbE breakout cluster port nodes
swp2s0-3	4x25GbE breakout cluster port nodes
swp3-14	40/100GbE cluster port nodes
swp15-16	100GbE Inter-Switch Link (ISL) ports

See the Hardware Universe for more information on switch ports.

Link-up delays with optical connections

If you are experiencing link-up delays of more than five seconds, Cumulus Linux 5.4 and later includes support for fast link-up. You can configure the links by using the `nv set` command as follows:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Show example

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Support for copper connections

The following configuration changes are required to fix this issue.

Cumulus Linux 4.4.3

1. Identify the name for each interface using 40GbE/100GbE copper cables:

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

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Add the following two lines to the `/etc/cumulus/switchd.conf` file for every port (swp<n>) that is using 40GbE/100GbE copper cables:
   - `interface.swp<n>.enable_media_depended_linkup_flow=TRUE`
   - `interface.swp<n>.enable_short_tuning=TRUE`

   For example:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
.
.
interface.swp3.enable_media_depended_linkup_flow=TRUE
interface.swp3.enable_short_tuning=TRUE
interface.swp4.enable_media_depended_linkup_flow=TRUE
interface.swp4.enable_short_tuning=TRUE
```

3. Restart the `switchd` service:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Confirm that the ports are up:

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

State  Name      Spd   MTU    Mode       LLDP               Summary
-----  --------- ----  -----  ---------- ------------------ --------
UP     swp3      100G  9216   Trunk/L2                      Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                      Master:
bridge(UP)
```

Cumulus Linux 5.x

1. Identify the name for each interface using 40GbE/100GbE copper cables:

```
cumulus@cumulus:mgmt:~$ nv show interface pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Configure the links using the `nv set` command as follows:
   - `nv set interface <interface-id> link fast-linkup on`
   - `nv config apply`
   - Reload the `switchd` service

   For example:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

3. Confirm that the ports are up:

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

State  Name      Spd   MTU    Mode        LLDP                Summary
-----  --------- ----  -----  ----------  ------------------  --------
UP     swp3      100G  9216   Trunk/L2                        Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                        Master:
bridge(UP)
```

See the Knowledge Base article SN2100 switch fails to connect using 40/100GbE copper cables for further details.

On Cumulus Linux 4.4.2, copper connections are not supported on SN2100 switches with X1151A NIC, X1146A NIC, or onboard 100GbE ports.
For example:

- AFF A800 on ports e0a and e0b
- AFF A320 on ports e0g and e0h

QSA adapter

When a QSA adapter is used to connect to the 10GbE/25GbE cluster ports on a platform, the link might not come up.

To resolve this issue, do the following:

- For 10GbE, manually set the swp1s0-3 link speed to 10000 and set auto-negotiation to off.
- For 25GbE, manually set the swp2s0-3 link speed to 25000 and set auto-negotiation to off.

When using 10GbE/25GbE QSA adapters, insert them in non-breakout 40GbE/100GbE ports (swp3-swp14). Do not insert the QSA adapter in a port that is configured for breakout.

Set interface speed on breakout ports

Depending on the transceiver in the switch port, you might need to set the speed on the switch interface to a fixed speed. If using 10GbE and 25GbE breakout ports, verify that auto-negotiation is off and set the interface speed on the switch.

Cumulus Linux 4.4.3

For example:

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

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

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

Check the interface and port status to verify that the settings are applied:

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

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

Cumulus Linux 5.x

For example:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3

link

  auto-negotiate        off                     off
off
  duplex                full                    full
full
  speed                 10G                     10G
10G
  fec                   auto                    auto
auto
  mtu                   9216                    9216
9216
[breakout]

  state                 up                      up
up
```

Check the interface and port status to verify that the settings are applied:

```
cumulus@cumulus:mgmt:~$ nv show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

What's next?

After you've reviewed your cabling and configuration requirements, you can cable the NS224 shelves as switch-attached storage.

Cable NS224 shelves as switch-attached storage

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

- Cable NS224 drive shelves through storage switches:

  Information for cabling switch-attached NS224 drive shelves

- Install your storage switches:

  AFF and FAS Switch Documentation

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

  NetApp Hardware Universe

Configure software

Software install workflow for NVIDIA SN2100 storage switches

To install and configure the software for a NVIDIA SN2100 switch, follow these steps:

Configure the switch

Configure the NVIDIA SN2100 switch.

Install Cumulus Linux in Cumulus mode

You can install the Cumulus Linux (CL) OS when the switch is running Cumulus Linux.

Install Cumulus Linux in ONIE mode

Alternatively, you can install the Cumulus Linux (CL) OS when the switch is running Cumulus Linux in ONIE mode.

Install the Reference Configuration File (RCF) script

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

Install the CSHM file

You can install the applicable configuration file for Ethernet switch health monitoring of NVIDIA cluster switches.

Reset the switch to factory defaults

Erase the SN2100 storage switch settings.

Configure the NVIDIA SN2100 switch

To configure the SN2100 switch, refer to NVIDIA's documentation.

Steps

1. Review the configuration requirements.
2. Follow the instructions in NVIDIA System Bring-Up..

What's next?

After you've configured your switches, you can install Cumulus Linux in Cumulus mode or install Cumulus Linux in ONIE mode.

Install Cumulus Linux in Cumulus mode

Follow this procedure to install Cumulus Linux (CL) OS when the switch is running in Cumulus mode.

> Cumulus Linux (CL) OS can be installed either when the switch is running Cumulus Linux or ONIE (see Install in ONIE mode).

Before you begin

Make sure that the following are available:

- Intermediate-level Linux knowledge.
- Familiarity with basic text editing, UNIX file permissions, and process monitoring. A variety of text editors are pre-installed, including `vi` and `nano`.
- Access to a Linux or UNIX shell. If you are running Windows, use a Linux environment as your command line tool for interacting with Cumulus Linux.
- The baud rate requirement must be set to 115200 on the serial console switch for NVIDIA SN2100 switch console access, as follows:
  - 115200 baud
  - 8 data bits
  - 1 stop bit
  - parity: none
  - flow control: none

About this task

Be aware of the following:

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

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

Example 1. Steps

Cumulus Linux 4.4.3

1. Log in to the switch.

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

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

2. Check the Cumulus Linux version: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

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

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

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

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

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

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

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

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

5. Set the date, time, time zone, and NTP server on the switch.
   a. Verify the current time zone:

```
cumulus@sw1:~$ cat /etc/timezone
```

   b. Update to the new time zone:

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

c. Verify your current time zone:

```
cumulus@switch:~$ date +%Z
```

d. To set the time zone using the guided wizard, run the following command:

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

e. Set the software clock according to the configured time zone:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Set the current value of the software clock to the hardware clock:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Add an NTP server if required:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>
iburst
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

h. Verify that `ntpd` is running on the system:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

i. Specify the NTP source interface. By default, the source interface that NTP uses is `eth0`. You can configure a different NTP source interface as follows:

```
cumulus@sw1:~$ net add time ntp source <src_int>
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

6. Install Cumulus Linux 4.4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

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

7. Reboot the NVIDIA SN2100 switch:

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

8. The installation starts automatically, and the following GRUB screen choices appear. Do **not** make any selections.
   - Cumulus-Linux GNU/Linux
   - ONIE: Install OS
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repeat steps 1 to 4 to log in.
10. Verify that the Cumulus Linux version is 4.4.3: `net show version`

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

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

```
sudo adduser --ingroup netedit admin
```

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

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

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

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

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

Cumulus Linux 5.4.0

1. Log in to the switch.

   First time log in to the switch requires username/password of **cumulus**/**cumulus** with `sudo`

privileges.

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

2. Check the Cumulus Linux version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.3.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

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

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

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

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

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

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

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

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

5. Set the time zone, date, time, and NTP server on the switch.
   a. Set the time zone:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Verify your current time zone:

```
cumulus@switch:~$ date +%Z
```

   c. To set the time zone using the guided wizard, run the following command:

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

   d. Set the software clock according to the configured time zone:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

   e. Set the current value of the software clock to the hardware clock:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Add an NTP server if required:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

See the Knowledge Base article NTP server configuration is not working with NVIDIA SN2100 switches for further details.

g. Verify that `ntpd` is running on the system:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Specify the NTP source interface. By default, the source interface that NTP uses is `eth0`. You can configure a different NTP source interface as follows:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Install Cumulus Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

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

7. Reboot the NVIDIA SN2100 switch:

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

8. The installation starts automatically, and the following GRUB screen choices appear. Do **not** make any selections.
   - Cumulus-Linux GNU/Linux
   - ONIE: Install OS
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repeat steps 1 to 4 to log in.
10. Verify that the Cumulus Linux version is 5.4.0: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational          applied              description
-------------------- -------------------- --------------------
hostname             cumulus              cumulus
build                Cumulus Linux 5.4.0  system build version
uptime               6 days, 13:37:36     system uptime
timezone             Etc/UTC              system time zone
```

11. Verify that the nodes each have a connection to each switch:

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

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ---------------------------------
-----------
eth0       100M   Mgmt        mgmt-sw1
Eth110/1/29
swp2s1     25G    Trunk/L2    node1
e0a
swp15      100G   BondMember  sw2
swp15
swp16      100G   BondMember  sw2
swp16
```

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

```
sudo adduser --ingroup netedit admin
```

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

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

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

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

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

13. Add additional user groups for the admin user to access `nv` commands:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user 'admin' to group 'nvshow' ...
     Adding user admin to group nvshow
     Done.
```

See NVIDIA User Accounts for more information.

Cumulus Linux 5.11.0

1. Log in to the switch.

   When you log in to the switch for the first time, it requires the username/password of **cumulus** /**cumulus** with `sudo` privileges.

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

2. Check the Cumulus Linux version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

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

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

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

```
cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

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

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

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

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

5. Set the time zone, date, time, and NTP server on the switch.
   a. Set the time zone:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Verify your current time zone:

```
cumulus@switch:~$ date +%Z
```

   c. To set the time zone using the guided wizard, run the following command:

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

d. Set the software clock according to the configured time zone:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

e. Set the current value of the software clock to the hardware clock:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Add an NTP server if required:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

See the Knowledge Base article NTP server configuration is not working with NVIDIA SN2100 switches for further details.

g. Verify that `ntpd` is running on the system:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Specify the NTP source interface. By default, the source interface that NTP uses is `eth0`. You can configure a different NTP source interface as follows:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Install Cumulus Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

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

7. Reboot the NVIDIA SN2100 switch:

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

8. The installation starts automatically, and the following GRUB screen choices appear. Do **not** make any selections.
   - Cumulus-Linux GNU/Linux
   - ONIE: Install OS
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Repeat steps 1 to 4 to log in.
10. Verify that the Cumulus Linux version is 5.11.0:

    `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied                 description
------------------- ----------------------- --------------------
build               Cumulus Linux 5.11.0
uptime              153 days, 2:44:16
hostname            cumulus                 cumulus
product-name        Cumulus Linux
product-release     5.11.0
platform            x86_64-mlnx_x86-r0
system-memory       2.76 GB used / 2.28 GB free / 7.47 GB total
swap-memory         0 Bytes used / 0 Bytes free / 0 Bytes total
health-status       not OK
date-time           2025-04-23 09:55:24
status              N/A
timezone            Etc/UTC
maintenance
  mode              disabled
  ports             enabled
version
  kernel            6.1.0-cl-1-amd64
  build-date        Thu Nov 14 13:06:38 UTC 2024
  image             5.11.0
  onie              2019.11-5.2.0020-115200
```

11. Verify that each node has a connection to each switch:

```
cumulus@sw1:mgmt:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ---------------------------------
-----------
eth0       100M   eth   mgmt-sw1
Eth110/1/14
swp2s1     25G    Trunk/L2    node1
e0a
swp1s1     10G    swp   sw2
e0a
swp9       100G   swp   sw3
e4a
swp10      100G   swp   sw4
e4a
swp15      100G   swp   sw5
swp15
swp16      100G   swp   sw6
swp16
```

See NVIDIA User Accounts for more information.

What's next?

After you've installed Cumulus Linux in Cumulus mode, you can install or upgrade the RCF script.

Install Cumulus Linux in ONIE mode

Follow this procedure to install Cumulus Linux (CL) OS when the switch is running in ONIE mode.

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

About this task

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

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

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

Steps

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

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

4. Reboot the SN2100 switch:

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

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

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

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

```
ifconfig eth0
```

Show example

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

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

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

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

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

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

```
ONIE:/ # route

  Kernel IP routing table

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

  Stopping: discover... done.
  Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-4.4.3-
mlx-amd64.bin ...
  Connecting to 10.60.132.97 (10.60.132.97:80)
  installer            100% |*|   552M  0:00:00 ETA
  ...
  ...
```

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

Show example

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

14. Verify the Cumulus Linux version:

```
net show version
```

Show example

```
cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3”
```

What’s next?

After you've installed Cumulus Linux in ONIE mode, you can install or upgrade the RCF script.

Install or upgrade the RCF script

Follow this procedure to install or upgrade the RCF script.

Before you begin

Before installing or upgrading the RCF script, make sure that the following are available on the switch:

- Cumulus Linux 4.4.3 is installed.
- IP address, subnet mask, and default gateway defined via DHCP or manually configured.

Current RCF script versions

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

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

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

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

Steps

1. Display the available interfaces on the SN2100 switch:

```
net show interface all
```

Show example

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

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

2. Copy the RCF python script to the switch:

```
admin@sw1:mgmt:~$ pwd
/home/cumulus
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.8-
Cluster
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.8-Cluster                  100% 8607   111.2KB/s
00:00
```

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

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

The RCF script completes the steps listed above.

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

4. Reapply any previous customizations to the switch configuration. Refer to Review cabling and configuration considerations for details of any further changes required.
5. Verify the configuration after the reboot:

```
net show interface all
```

Show example

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

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

```
DN     swp14     N/A   9216   Trunk/L2                    Master:
bridge(UP)
UP     swp15     N/A   9216   BondMember                  Master:
bond_15_16(UP)
UP     swp16     N/A   9216   BondMember                  Master:
bond_15_16(UP)
...
...

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

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

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

6. Verify information for the transceiver in the interface:

```
net show interface pluggables
```

Show example

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

7. Verify that the nodes each have a connection to each switch:

   ```
   net show lldp
   ```

   Show example

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

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

8. Verify the health of cluster ports on the cluster.
   a. Verify that e0d ports are up and healthy across all nodes in the cluster:

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

Show example

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

Node: node1

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

Node: node2

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

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

Show example

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

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


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                         cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                         cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

What's next?

After you've installed or upgraded the RCF, you can install the CSHM file.

Install the Ethernet Switch Health Monitor configuration file

Follow this procedure to install the applicable configuration file for Ethernet switch health monitoring of NVIDIA cluster switches.
Supported models are:

- MSN2100-CB2FC
- MSN2100-CB2RC
- X190006-PE
- X190006-PI

This installation procedure applies to ONTAP 9.10.1 and later.

Before you begin

- Verify that you need to download the configuration file by running `system switch ethernet show` and checking if **OTHER** is shown for your model.

  If your model is still showing **OTHER** after applying the configuration file, contact NetApp support.

- Make sure that the ONTAP cluster is up and running.
- Enable SSH to use all of the features available in CSHM.
- Clear the `/mroot/etc/cshm_nod/nod_sign/` directory on all nodes:
  a. Enter the nodeshell:

     ```
     system node run -node <name>
     ```

  b. Change to advanced privilege:

     ```
     priv set advanced
     ```

  c. List the configuration files in the `/etc/cshm_nod/nod_sign` directory. If the directory exists and contains configuration files, it lists the file names.

     ```
     ls /etc/cshm_nod/nod_sign
     ```

  d. Delete all configuration files corresponding to your connected switch models.

     If you are unsure, remove all configuration files for the supported models listed above, then download and install the latest configuration files for those same models.

     ```
     rm /etc/cshm_nod/nod_sign/<filename>
     ```

  e. Confirm that the deleted configuration files are no longer in the directory:

     ```
     ls /etc/cshm_nod/nod_sign
     ```

Steps

1. Download the Ethernet switch health monitor configuration zip file based on the corresponding ONTAP release version. This file is available from the NVIDIA Ethernet switches page.

a. On the NVIDIA SN2100 Software download page, select **Nvidia CSHM File**.

b. On the Caution/Must read page, select the check box to agree.

c. On the End User License Agreement page, select the check box to agree and click **Accept & Continue**.

d. On the Nvidia CSHM File - Download page, select the applicable configuration file. The following files are available:

ONTAP 9.15.1 and later

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 through 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

2. Upload the applicable zip file to your internal web server.
3. Access the advanced mode setting from one of the ONTAP systems in the cluster.

```
set -privilege advanced
```

4. Run the switch health monitor configure command.

```
cluster1::> system switch ethernet configure-health-monitor
```

5. Verify that the command output ends with the following text for your ONTAP version:

ONTAP 9.15.1 and later

Ethernet switch health monitoring installed the configuration file.

ONTAP 9.11.1 through 9.14.1

SHM installed the configuration file.

ONTAP 9.10.1

CSHM downloaded package processed successfully.

If an error occurs, contact NetApp support.

6. Wait up to twice the Ethernet switch health monitor polling interval, found by running `system switch ethernet polling-interval show`, before completing the next step.

7. Run the command `system switch ethernet configure-health-monitor show` on the ONTAP system and make sure that the cluster switches are discovered with the monitored field set to **True** and the serial number field not showing **Unknown**.

```
cluster1::> system switch ethernet configure-health-monitor show
```

What's next?

After you've installed the CSHM file, you can configure switch health monitoring.

Reset the SN2100 storage switch to factory defaults

To reset the SN2100 storage switch to factory defaults:

- For Cumulus Linux 5.10 and earlier, you apply the Cumulus image.
- For Cumulus Linux 5.11 and later, you use the `nv action reset system factory-default` command.

About this task

- You must be connected to the switch using the serial console.
- You must have the root password for sudo access to the commands.

For more information about installing Cumulus Linux, see Software install workflow for NVIDIA SN2100 switches.

Example 2. Steps

Cumulus Linux 5.10 and earlier

1. From the Cumulus console, download and queue the switch software installation with the command `onie-install -a -i` followed by the file path to the switch software, for example:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. The installer starts the download. Type **y** when prompted to confirm the installation when the image is downloaded and verified.
3. Reboot the switch to install the new software.

   `sudo reboot`

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

> The switch reboots and enters the switch software installation which takes some time. When the installation is complete, the switch reboots and remains at the `log-in` prompt.

Cumulus Linux 5.11 and later

1. To reset the switch to the factory defaults and remove all configuration, system files, and log files, run:

   `nv action reset system factory-default`

   For example:

```
cumulus@switch:~$ nv action reset system factory-default

This operation will reset the system configuration, delete the log
files and reboot the switch.
Type [y] continue.
Type [n] to abort.
Do you want to continue? [y/n] y
```

See the NVIDIA Factory Reset documentation for further details.

What's next

After you've reset your switches, you can reconfigure them as needed.

Migrate switches

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

You can migrate older Cisco switches for an ONTAP cluster to NVIDIA SN2100 storage switches. This is a non-disruptive procedure.

Review requirements

The following storage switches are supported:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- See the Hardware Universe for full details of supported ports and their configurations.

Before you begin

Make sure that you have the following:

- The existing cluster is properly set up and functioning.
- All storage ports are in the up state to ensure nondisruptive operations.
- The NVIDIA SN2100 storage switches are configured and operating under the proper version of Cumulus Linux installed with the reference configuration file (RCF) applied.
- The existing storage network configuration has the following:
  - A redundant and fully functional NetApp cluster using both older Cisco switches.
  - Management connectivity and console access to both the older Cisco switches and the new switches.
  - All cluster LIFs in the up state with the cluster LIFs are on their home ports.
  - ISL ports enabled and cabled between the older Cisco switches and between the new switches.
- See the Hardware Universe for full details of supported ports and their configurations.
- Some of the ports are configured on NVIDIA SN2100 switches to run at 100 GbE.
- You have planned, migrated, and documented 100 GbE connectivity from nodes to NVIDIA SN2100 storage switches.

Migrate the switches

About the examples

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

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

- The existing Cisco Nexus 9336C-FX2 storage switches are *S1* and *S2*.
- The new NVIDIA SN2100 storage switches are *sw1* and *sw2*.
- The nodes are *node1* and *node2*.
- The cluster LIFs are *node1_clus1* and *node1_clus2* on node 1, and *node2_clus1* and *node2_clus2* on node 2 respectively.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The network ports used in this procedure are *e5a* and *e5b*.

- Breakout ports take the format: swp1s0-3. For example four breakout ports on swp1 are *swp1s0*, *swp1s1*, *swp1s2*, and *swp1s3*.
- Switch S2 is replaced by switch sw2 first and then switch S1 is replaced by switch sw1.
  - Cabling between the nodes and S2 are then disconnected from S2 and reconnected to sw2.
  - Cabling between the nodes and S1 are then disconnected from S1 and reconnected to sw1.

Step 1: Prepare for migration

1. If AutoSupport is enabled, suppress automatic case creation by invoking an AutoSupport message:

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

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

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

   `set -privilege advanced`

   The advanced prompt (*>) appears.

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

   Each port should display enabled for `Status`.

Step 2: Configure cables and ports

1. Display the network port attributes:

   `storage port show`

   Show example

```
cluster1::*> storage port show
                                  Speed                      VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online      30
               e0d  ENET  storage    0   enabled  offline     30
               e5a  ENET  storage    0   enabled  offline     30
               e5b  ENET  storage  100   enabled  online      30
node2
               e0c  ENET  storage  100   enabled  online      30
               e0d  ENET  storage    0   enabled  offline     30
               e5a  ENET  storage    0   enabled  offline     30
               e5b  ENET  storage  100   enabled  online      30
cluster1::*>
```

2. Verify that the storage ports on each node are connected to existing storage switches in the following way (from the nodes' perspective) using the command:

   ```
   network device-discovery show -protocol lldp
   ```

   Show example

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

3. On switch S1 and S2, make sure that the storage ports and switches are connected in the following way (from the switches' perspective) using the command:

   ```
   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     Holdtime    Capability
Port ID
node1                 Eth1/1         121         S
e0c
node2                 Eth1/2         121         S
e0c
SHFGD1947000186       Eth1/10        120         S
  e0a
SHFGD1947000186       Eth1/11        120         S
  e0a
SHFGB2017000269       Eth1/12        120         S
  e0a
SHFGB2017000269       Eth1/13        120         S
  e0a

S2# show lldp neighbors

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS
Cable Device,
                  (W) WLAN Access Point, (P) Repeater, (S) Station
(O) Other

Device-ID             Local Intf     Holdtime    Capability
Port ID
node1                 Eth1/1         121         S
e5b
node2                 Eth1/2         121         S
e5b
SHFGD1947000186       Eth1/10        120         S
 e0b
SHFGD1947000186       Eth1/11        120         S
 e0b
SHFGB2017000269       Eth1/12        120         S
 e0b
SHFGB2017000269       Eth1/13        120         S
 e0b
```

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

Show example

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

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

Show example

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

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

```
network device-discovery show -protocol lldp
```

Show example

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

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

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

8. Verify the network port attributes:

```
storage port show
```

Show example

```
cluster1::*> storage port show
                                  Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
node2
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
cluster1::*>
```

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

   `net show interface`

Show example

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

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

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

Show example

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

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

Show example

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

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

    `network device-discovery show -protocol lldp`

    Show example

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

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

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

Step 3: Verify the configuration

1. Verify the final configuration:

   `storage port show`

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

Show example

```
cluster1::*> storage port show
                                  Speed                      VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
node2
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
cluster1::*>
```

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

   `net show interface`

Show example

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

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

3. Verify that both nodes each have one connection to each switch:

   ```
   net show lldp
   ```

Show example

The following example shows the appropriate results for both switches:

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

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

1. Change the privilege level back to admin:

   ```
   set -privilege admin
   ```

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

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

What's next?

After you've migrated your switches, you can configure switch health monitoring.

Replace a NVIDIA SN2100 storage switch

You can replace a defective NVIDIA SN2100 storage switch. This is a nondisruptive procedure.

Before you begin

Before installing the Cumulus software and RCFs on a NVIDIA SN2100 storage switch, ensure that:

- Your system can support NVIDIA SN2100 storage switches.

- You have downloaded the applicable RCFs.

The Hardware Universe provides full details of supported ports and their configurations.

The existing network configuration must have the following characteristics:

- Complete all troubleshooting steps to confirm you need to replace your switch.
- Ensure management connectivity exists on both switches.

> Make sure that all troubleshooting steps have been completed to confirm that your switch needs replacing.

The replacement NVIDIA SN2100 switch must have the following characteristics:

- Management network connectivity is functional.
- You can access the replacement switch using the console.
- The appropriate RCF and Cumulus operating system image is loaded onto the switch.
- Initial customization of the switch is complete.

Procedure summary

This procedure replaces the second NVIDIA SN2100 storage switch sw2 with the new NVIDIA SN2100 switch nsw2. The two nodes are node1 and node2.

Steps to complete:

- Confirm the switch to be replaced is sw2.
- Disconnect the cables from switch sw2.
- Reconnect the cables to switch nsw2.
- Verify all device configurations on switch nsw2.

Steps

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

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

   x is the duration of the maintenance window in hours.

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

   ```
   set -privilege advanced
   ```

3. Check the health status of storage node ports to confirm connection to storage switch S1:

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

Show example

```
cluster1::*> storage port show -port-type ENET
                                  Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e3a  ENET  storage 100    enabled  online       30
               e3b  ENET  storage   0    enabled  offline      30
               e7a  ENET  storage   0    enabled  offline      30
               e7b  ENET  storage 100    enabled  online       30
node2
               e3a  ENET  storage 100    enabled  online       30
               e3b  ENET  storage   0    enabled  offline      30
               e7a  ENET  storage   0    enabled  offline      30
               e7b  ENET  storage 100    enabled  online       30
cluster1::*>
```

4. Verify that storage switch sw1 is available:

   `network device-discovery show -protocol lldp`

Show example

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1/lldp
            e0M    sw1 (00:ea:bd:68:6a:e8)   Eth1/46           -
            e0b    sw2 (6c:b2:ae:5f:a5:b2)   Ethernet1/16      -
            e0c    SHFFG1827000286 (d0:39:ea:1c:16:92)
                                             e0a               -
            e0e    sw3 (6c:b2:ae:5f:a5:ba)   Ethernet1/18      -
            e0f    SHFFG1827000286 (00:a0:98:fd:e4:a9)
                                             e0b               -
            e0g    sw4 (28:ac:9e:d5:4a:9c)   Ethernet1/11      -
            e0h    sw5 (6c:b2:ae:5f:a5:ca)   Ethernet1/22      -
            e1a    sw6 (00:f6:63:10:be:7c)   Ethernet1/33      -
            e1b    sw7 (00:f6:63:10:be:7d)   Ethernet1/34      -
            e2a    sw8 (b8:ce:f6:91:3d:88)   Ethernet1/35      -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

5. Run the `net show interface` command on the working switch to confirm that you can see both nodes and all shelves:

   `net show interface`

Show example

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

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e3a)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e3a)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP))
...
...
```

6. Verify the shelf ports in the storage system:

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

Show example

```
cluster1::*> storage shelf port show -fields remote-device, remote-
port
shelf   id  remote-port   remote-device
-----   --  -----------   -------------
3.20    0   swp3          sw1
3.20    1   -             -
3.20    2   swp4          sw1
3.20    3   -             -
3.30    0   swp5          sw1
3.20    1   -             -
3.30    2   swp6          sw1
3.20    3   -             -
cluster1::*>
```

7. Remove all cables attached to storage switch sw2.
8. Reconnect all cables to the replacement switch nsw2.
9. Recheck the health status of the storage node ports:

   `storage port show -port-type ENET`

   Show example

```
cluster1::*> storage port show -port-type ENET
                                  Speed                       VLAN
Node              Port Type  Mode    (Gb/s) State    Status      ID
----------------- ---- ----- ------- ------ -------- --------- ----
node1
                  e3a  ENET  storage 100    enabled  online      30
                  e3b  ENET  storage   0    enabled  offline     30
                  e7a  ENET  storage   0    enabled  offline     30
                  e7b  ENET  storage 100    enabled  online      30
node2
                  e3a  ENET  storage 100    enabled  online      30
                  e3b  ENET  storage   0    enabled  offline     30
                  e7a  ENET  storage   0    enabled  offline     30
                  e7b  ENET  storage 100    enabled  online      30
cluster1::*>
```

10. Verify that both switches are available:

    `net device-discovery show -protocol lldp`

Show example

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1/lldp
            e0M    sw1 (00:ea:bd:68:6a:e8)   Eth1/46           -
            e0b    sw2 (6c:b2:ae:5f:a5:b2)   Ethernet1/16      -
            e0c    SHFFG1827000286 (d0:39:ea:1c:16:92)
                                             e0a               -
            e0e    sw3 (6c:b2:ae:5f:a5:ba)   Ethernet1/18      -
            e0f    SHFFG1827000286 (00:a0:98:fd:e4:a9)
                                             e0b               -
            e0g    sw4 (28:ac:9e:d5:4a:9c)   Ethernet1/11      -
            e0h    sw5 (6c:b2:ae:5f:a5:ca)   Ethernet1/22      -
            e1a    sw6 (00:f6:63:10:be:7c)   Ethernet1/33      -
            e1b    sw7 (00:f6:63:10:be:7d)   Ethernet1/34      -
            e2a    sw8 (b8:ce:f6:91:3d:88)   Ethernet1/35      -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

11. Verify the shelf ports in the storage system:

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

Show example

```
cluster1::*> storage shelf port show -fields remote-device, remote-
port
shelf   id    remote-port     remote-device
-----   --    -----------     -------------
3.20    0     swp3            sw1
3.20    1     swp3            nsw2
3.20    2     swp4            sw1
3.20    3     swp4            nsw2
3.30    0     swp5            sw1
3.20    1     swp5            nsw2
3.30    2     swp6            sw1
3.20    3     swp6            nsw2
cluster1::*>
```

12. Change the privilege level back to admin:

    ```
    set -privilege admin
    ```

13. 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?

After you've replaced your switches, you can configure switch health monitoring.