Configure the software

Install and maintain

NetApp
March 06, 2026

Table of Contents

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.

Prompt	Response
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.
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.

Copyright information

Trademark information