



## Configure the software

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/us-en/ontap-systems-switches/switch-cisco-9336c-fx2-storage/configure-software-overview-9336c-storage.html> on February 13, 2026. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Table of Contents

Configure the software . . . . .	1
Software install workflow for Cisco Nexus 9336C-FX2 and 9336C-FX2-T storage switches . . . . .	1
Configure the 9336C-FX2 and 9336C-FX2-T storage switches . . . . .	1
Prepare to install or upgrade NX-OS software and RCF . . . . .	4
Install or upgrade the NX-OS software . . . . .	10
Review requirements . . . . .	10
Install the software . . . . .	11
Install or upgrade the RCF . . . . .	33
Install or upgrade the Reference Configuration File (RCF) overview . . . . .	33
Install the Reference Configuration File . . . . .	35
Upgrade your Reference Configuration File (RCF) . . . . .	46
Verify your SSH configuration . . . . .	55
Reset the 9336C-FX2 and 9336C-FX2-T storage switches to factory defaults . . . . .	57

# 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 cluster network and management network RCFs downloaded from the NetApp Support Site at [mysupport.netapp.com](http://mysupport.netapp.com). All Cisco cluster network and management network switches arrive with the standard Cisco factory-default configuration. These switches also have the current version of the NX-OS software but do not have the RCFs loaded.
- Required switch documentation. See [Required documentation](#) for more information.

## Steps

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

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

Prompt	Response
Abort Auto Provisioning and continue with normal setup? (yes/no)	Respond with <b>yes</b> . The default is no.
Do you want to enforce secure password standard? (yes/no)	Respond with <b>yes</b> . 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 <b>yes</b> 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 <b>no</b> .
Configure read-only SNMP community string? (yes/no)	Respond with <b>no</b> . The default is no.
Configure read-write SNMP community string? (yes/no)	Respond with <b>no</b> . 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 <b>yes</b> (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 <b>yes</b> . At the IPv4 address of the default-gateway: prompt, enter your default_gateway.
Configure advanced IP options? (yes/no)	Respond with <b>no</b> . The default is no.
Enable the telnet service? (yes/no)	Respond with <b>no</b> . The default is no.
Enabled SSH service? (yes/no)	<p>Respond with <b>yes</b>. The default is yes.</p> <p> SSH is recommended when using Ethernet Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security.</p>
Enter the type of SSH key you want to generate (dsa/rsa/rsa1).	The default is <b>rsa</b> .
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 <b>no</b> . The default is no.
Configure default interface layer (L3/L2)	Respond with <b>L2</b> . The default is L2.
Configure default switch port interface state (shut/noshut)	Respond with <b>noshut</b> . The default is noshut.
Configure CoPP system profile (strict/moderate/lenient/dense)	Respond with <b>strict</b> . The default is strict.
Would you like to edit the configuration? (yes/no)	<p>You should see the new configuration at this point. Review and make any necessary changes to the configuration you just entered.</p> <p>Respond with <b>no</b> at the prompt if you are satisfied with the configuration. Respond with <b>yes</b> if you want to edit your configuration settings.</p>
Use this configuration and save it? (yes/no)	<p>Respond with <b>yes</b> to save the configuration. This automatically updates the kickstart and system images.</p> <p> 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.</p>

2. Verify the configuration choices you made in the display that appears at the end of the setup, and make sure that you save the configuration.
3. Check the version on the cluster network switches, and if necessary, download the NetApp-supported version of the software to the switches from the [Cisco software download](#) page.

#### What's next?

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

#### About this task

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

#### Steps

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



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

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

```
set -privilege advanced
```

The advanced prompt (`*>`) appears.

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

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

## Show example

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

Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----  

cluster1-02/lldp
      e0a    cs1          Eth1/2      N9K-
C9336C
      e0b    cs2          Eth1/2      N9K-
C9336C
cluster1-01/lldp
      e0a    cs1          Eth1/1      N9K-
C9336C
      e0b    cs2          Eth1/1      N9K-
C9336C

4 entries were displayed.
```

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

- a. Display the network port attributes:

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

## Show example

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

Node: cluster1-02

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

Node: cluster1-01

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

4 entries were displayed.
```

### b. Display information about the LIFs:

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

### Show example

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

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

4 entries were displayed.
```

5. Verify the connectivity of the remote cluster interfaces:

## ONTAP 9.9.1 and later

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date          LIF          LIF
Loss
----- ----- ----- -----
```

node1	3/5/2024 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-
clus1	none		
	3/5/2024 19:21:20 -06:00	cluster1-01_clus2	cluster1-
02_clus2	none		
node2	3/5/2024 19:21:18 -06:00	cluster1-02_clus2	cluster1-
01_clus1	none		
	3/5/2024 19:21:20 -06:00	cluster1-02_clus2	cluster1-
01_clus2	none		

## All ONTAP releases

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

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

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

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

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

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

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

## Show example

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

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

## 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 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 do the following:

- Run the `show install all impact nxos bootflash:<image_name>.bin` command on the switch to review the impact of installing or upgrading the new NX-OS software image. It verifies the image integrity, checks for necessary reboots, evaluates hardware compatibility, and confirms sufficient space.
- Review the release notes for the target NX-OS software version to check for any specific requirements.
- Verify that you have a current backup of the switch configuration.
- Verify that you have a fully functioning cluster (no errors in the logs or similar issues).

### Suggested documentation

- [Cisco Ethernet switch page](#)

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

- [Software Upgrade and downgrade guides](#)

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

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

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

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

### About the examples

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

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

## Install the software

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

### Steps

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

#### Show example

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

```
cs2# ping 172.19.2.1 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. Display the cluster ports on each node that are connected to the cluster switches:

```
network device-discovery show
```

## Show example

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

-----
-----
cluster1-01/cdp
    e0a    cs1
C9336C-FX2
    e0b    cs2
C9336C-FX2
cluster1-02/cdp
    e0a    cs1
C9336C-FX2
    e0b    cs2
C9336C-FX2
cluster1-03/cdp
    e0a    cs1
C9336C-FX2
    e0b    cs2
C9336C-FX2
cluster1-04/cdp
    e0a    cs1
C9336C-FX2
    e0b    cs2
C9336C-FX2
cluster1::*
```

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

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

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

## Show example

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```

Node: cluster1-04

Ignore

          Speed (Mbps)

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

```

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

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

**Show example**

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

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

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

**Show example**

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                  Type          Address
Model
-----
-----
cs1                   cluster-network 10.233.205.90
N9K-C9336C-FX2
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    9.3(5)
    Version Source: CDP

cs2                   cluster-network 10.233.205.91
N9K-C9336C-FX2
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    9.3(5)
    Version Source: CDP
cluster1::*>
```

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

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

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

Show example

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

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

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

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

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

```
show version
```

## Show example

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own

licenses, such as open source. This software is provided "as is,"
and unless

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

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

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

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

### Software

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

### Hardware

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

Processor Board ID FOC20291J6K
```

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

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

  plugin
    Core Plugin, Ethernet Plugin

  Active Package(s) :

  cs2#
```

## 8. Install the NX-OS image.

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

## Show example

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

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

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

Verifying image type.
[] 100% -- SUCCESS

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

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

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

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

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

Images will be upgraded according to following table:

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

```
Switch will be reloaded for disruptive upgrade.

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

Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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

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

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

```
show version
```

## Show example

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.

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

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

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

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

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

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

```
Reason: Reset due to upgrade
```

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

10. Upgrade the EPLD image and reboot the switch.

**Show example**

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

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

```
cs2# 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 Required	Type	EPLD	Running-Version	New-Version	Upg-
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

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

**Show example**

```
cs2# show version module 1 epld

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

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

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

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

## Show example

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04
```

```
Ignore
```

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

```
8 entries were displayed.
```

b. Verify the switch health from the cluster.

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

## Show example

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

-----
-----
cluster1-01/cdp
    e0a    cs1                      Ethernet1/7
N9K-C9336C-FX2
    e0b    cs2                      Ethernet1/7
N9K-C9336C-FX2
cluster01-2/cdp
    e0a    cs1                      Ethernet1/8
N9K-C9336C-FX2
    e0b    cs2                      Ethernet1/8
N9K-C9336C-FX2
cluster01-3/cdp
    e0a    cs1                      Ethernet1/1/1
N9K-C9336C-FX2
    e0b    cs2                      Ethernet1/1/1
N9K-C9336C-FX2
cluster1-04/cdp
    e0a    cs1                      Ethernet1/1/2
N9K-C9336C-FX2
    e0b    cs2                      Ethernet1/1/2
N9K-C9336C-FX2

cluster1::*> system cluster-switch show -is-monitoring-enabled -operational true
Switch                  Type          Address
Model

-----
-----
cs1                    cluster-network  10.233.205.90
N9K-C9336C-FX2
    Serial Number: FOCXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    9.3(5)
    Version Source: CDP

cs2                    cluster-network  10.233.205.91
```

```

N9K-C9336C-FX2
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
    Software, Version
        9.3(5)
    Version Source: CDP

2 entries were displayed.

```

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

```

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

```

13. Verify that the cluster is healthy:

```
cluster show
```

#### Show example

```

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

```

14. Repeat steps 6 to 13 to install the NX-OS software on switch cs1.
15. Verify the connectivity of the remote cluster interfaces before enabling auto-revert on the cluster LIFs:

## ONTAP 9.9.1 and later

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date                      LIF          LIF
Loss
-----
-----
cluster1-01
      3/5/2022 19:21:18 -06:00  cluster1-01_clus2  cluster1-02-
clus1    none
      3/5/2022 19:21:20 -06:00  cluster1-01_clus2  cluster1-
02_clus2  none
cluster1-02
      3/5/2022 19:21:18 -06:00  cluster1-02_clus2  cluster1-
01_clus1  none
      3/5/2022 19:21:20 -06:00  cluster1-02_clus2  cluster1-
01_clus2  none
```

## All ONTAP releases

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

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

```

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

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

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

```

16. Enable auto-revert on the cluster LIFs.

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

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

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

## Show example

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

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

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

## What's next?

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 configurations

The following table describes the RCFs available for different configurations. Choose the RCF applicable to your configuration. See [Cisco Ethernet Switches](#) for more information.

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

RCF name	Description
2-Cluster-HA-Breakout	Supports twoONTAP clusters with at least eight nodes, including nodes that use shared Cluster+HA ports.
4-Cluster-HA-Breakout	Supports fourONTAP clusters with at least four nodes, including nodes that use shared Cluster+HA ports.
1-Cluster-HA	All ports are configured for 40/100GbE. Supports shared cluster/HA traffic on ports. Required for AFF A320, AFF A250, and FAS500f systems. Additionally, all ports can be used as dedicated cluster ports.
1-Cluster-HA-Breakout	Ports are configured for 4x10GbE breakout, 4x25GbE breakout (RCF 1.6+ on 100GbE switches), and 40/100GbE. Supports shared cluster/HA traffic on ports for nodes that use shared cluster/HA ports: AFF A320, AFF A250, and FAS500f systems. Additionally, all ports can be used as dedicated cluster ports.
Cluster-HA-Storage	Ports are configured for 40/100GbE for Cluster+HA, 4x10GbE breakout for Cluster and 4x25GbE breakout for Cluster+HA, and 100GbE for each storage HA pair.
Cluster	Two flavors of RCF with different allocations of 4x10GbE ports (breakout) and 40/100GbE ports. All FAS and AFF nodes are supported, except for AFF A320, AFF A250, and FAS500f systems.
Storage	All ports are configured for 100GbE NVMe storage connections.

### Available RCFs

The following table lists the available RCFs for 9336C-FX2 and 9336C-FX2-T switches. Choose the applicable RCF version for your configuration. See [Cisco Ethernet Switches](#) for more information.

RCF name
Cluster-HA-Breakout RCF 1.xx
Cluster-HA-Storage RCF 1.xx
Storage RCF 1.xx
MultiCluster-HA RCF 1.xx

## 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 cs1 and cs2.
- The node names are node1-01, node1-02, node1-03, and node1-04.
- The cluster LIF names are node1-01\_clus1, node1-01\_clus2, node1-02\_clus1, node1-02\_clus2, node1-03\_clus1, node1-03\_clus2, node1-04\_clus1, and node1-04\_clus2.
- The `cluster1::*` prompt indicates the name of the cluster.

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 cs1 and switch cs2 are powered up and the initial switch setup is complete (the Management IP address and SSH is set up).
- The desired NX-OS version has been installed.

- ONTAP node cluster ports are not connected.

## Step 1: Install the RCF on the switches

1. Login to switch cs1 using SSH or by using a serial console.
2. Copy the RCF to the bootflash of switch cs1 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP.

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

### Show example

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

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Storage.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

3. Apply the RCF previously downloaded to the bootflash.

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

### Show example

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

```
cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-
commands
```

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

## Show example

```
cs1# show banner motd

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

### 5. Verify that the RCF is the correct newer version:

```
show running-config
```

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

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

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

### 6. 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.

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

### 8. Save basic configuration details to the write\_erase.cfg file on the bootflash.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg
```

```
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. When installing RCF version 1.12 and later, run the following commands:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >> bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region egr-racl 1024" >> bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region ing-12-qos 1280" >> 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.

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

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

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

```
cs1# write erase
```

Warning: This command will erase the startup-configuration.

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

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

```
cs1# copy bootflash:write_erase.cfg startup-config
```

13. Reboot switch cs1.

```
cs1# reload
```

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

14. Repeat steps 1 through 13 on switch cs2.

15. Connect the cluster ports of all nodes in the ONTAP cluster to switches cs1 and cs2.

## Step 2: Verify the switch connections

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

```
show interface brief
```

## Show example

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

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

```
show vlan brief
```

```
show interface trunk
```

**Show example**

```
cs1# show vlan brief
```

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

```
cs1# show interface trunk
```

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

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

#### Port Vlans Allowed on Trunk

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

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

---

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

---

-----

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

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

---



---



---

Port                    STP Forwarding

---



---

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

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

---

---

Port                    Vlans in spanning tree forwarding state and not pruned

---

---

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

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

Eth1/36	Feature VTP is not enabled
none	



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

### Step 3: Set up your ONTAP cluster

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

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

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

#### What's next?

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.



No operational inter-switch link (ISL) is needed during this procedure. This is by design because RCF version changes can affect ISL connectivity temporarily. To ensure non-disruptive cluster operations, the following procedure migrates all of the cluster LIFs to the operational partner switch while performing the steps on the target switch.



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
-----  -----  -----
-----  -----
node1-01/cdp
      e3a    cs1                      Ethernet1/7      N9K-
C9336C
      e3b    cs2                      Ethernet1/7      N9K-
C9336C
node1-02/cdp
      e3a    cs1                      Ethernet1/8      N9K-
C9336C
      e3b    cs2                      Ethernet1/8      N9K-
C9336C
.
.
.
```

4. 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
```

Node	Port	Type	Mode	Speed		
				(Gb/s)	State	Status
<hr/>						
node1-01	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
node1-02	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
.						
.						
.						

## 5. Disable auto-revert on the cluster LIFs.

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

## Step 2: Configure ports

### 1. On switch cs1, shut down the ports connected to all the nodes.

```
cs1> enable
cs1# configure
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(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.

### 2. Verify that the cluster LIFs have failed over to the ports hosted on switch cs1. This might take a few seconds.

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

### Show example

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

          Logical          Status      Network      Current
Current Is
Vserver      Interface      Admin/Oper Address/Mask      Node
Port        Home
-----  -----  -----
-----  -----  -----
Cluster
e7a          node1-01_clus1  up/up      169.254.36.44/16  node1-01
          true
e7b          node1-01_clus2  up/up      169.254.7.5/16   node1-01
          true
          node1-02_clus1  up/up      169.254.197.206/16 node1-02
e7a          true
          node1-02_clus2  up/up      169.254.195.186/16 node1-02
e7b          true
          node1-03_clus1  up/up      169.254.192.49/16  node1-03
e7a          true
          node1-03_clus2  up/up      169.254.182.76/16  node1-03
e7b          true
          node1-04_clus1  up/up      169.254.59.49/16   node1-04
e7a          true
          node1-04_clus2  up/up      169.254.62.244/16 node1-04
e7b          true

8 entries were displayed.
```

### 3. Verify that the cluster is healthy:

```
cluster show
```

## Show example

```
cluster1::*> cluster show
Node          Health  Eligibility  Epsilon
-----
node1-01      true    true         false
node1-02      true    true         false
node1-03      true    true         true
node1-04      true    true         false

4 entries were displayed.
```

4. 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
```

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

5. 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

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

6. When upgrading to RCF version 1.12 and later, run the following commands: `cs1# echo "hardware access-list tcam region ing-racl 1024" >> bootflash:write_erase.cfg`

```
cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280 >>
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.

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

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

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

```
cs1# write erase
```

Warning: This command will erase the startup-configuration.

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

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

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Reboot the switch:

```
cs1# reload
```

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

11. 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.

12. Copy the RCF to the bootflash of switch cs1 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP.

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

#### Show example

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

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Storage.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

13. 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.

[OS Command Reference](#) guides.

This example shows the RCF file `NX9336C-FX2-RCF-v1.13-1-Storage.txt` being installed on switch `cs1`:

```
cs1# copy Nexus_9336C_RCF_v1.6-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.

14. 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.

15. Reapply any previous customizations to the switch configuration.

16. 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.

```
cs1# copy running-config startup-config
```

```
[] 100% Copy complete
```

17. Reboot switch `cs1`. You can ignore the “cluster switch health monitor” alerts and “cluster ports down” events reported on the nodes while the switch reboots.

```
cs1# reload
```

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

18. 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
```

Node	Port	Type	Mode	Speed		
				(Gb/s)	State	Status
node1-01	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
node1-02	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
.						
.						
.						

19. Verify that the cluster is healthy:

```
cluster show
```

**Show example**

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

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

20. Repeat steps 4 to 19 on switch cs2.

21. Enable auto-revert on the cluster LIFs.

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

### Step 3: Verify the cluster network configuration and cluster health

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

```
show interface brief
```

2. Verify that the expected nodes are still connected:

```
show cdp neighbors
```

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

```
show vlan brief
```

```
show interface trunk
```

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

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

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

```
network interface revert -vserver vserver_name -lif <lif-name>
```

5. Verify that the cluster is healthy:

```
cluster show
```

6. Verify the connectivity of the remote cluster interfaces:

- a. You can use the `network interface check cluster-connectivity show` command to display the details of an accessibility check for cluster connectivity:

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

- b. Alternatively, you can use the `cluster ping-cluster -node <node-name>` command to check the connectivity:

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

### 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 cluster 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
AAAAB3NzaC1yc2EAAAQABAAAAgQDiNrD52Q586wTGJjFAbjB1FaA23EpDrZ2sDCew
17nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpz07+YCDsrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIBmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
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
```

```
(cs2) # 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
```

```
(cs2) # 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

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

## Trademark information

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