



# **Install NX-OS software and RCFs on Cisco Nexus 3232C cluster switches**

Cluster and storage switches

NetApp  
November 03, 2022

This PDF was generated from <https://docs.netapp.com/us-en/ontap-systems-switches/switch-cisco-3232c/task-install-the-nx-os-software-3232c-cluster-switch.html> on November 03, 2022. Always check docs.netapp.com for the latest.

# Table of Contents

- Install NX-OS software and RCFs on Cisco Nexus 3232C cluster switches . . . . . 1
  - Install the NX-OS software . . . . . 6
  - Install the Reference Configuration File (RCF) . . . . . 13

# Install NX-OS software and RCFs on Cisco Nexus 3232C cluster switches

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

## Before you begin

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

- The cluster must be fully functioning (there should be no errors in the logs or similar -ssues).
- You must have checked or set your desired boot configuration in the RCF to reflect the desired boot images if you are installing only NX-OS and keeping your current RCF version.
- If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is instantiated on future reboots.
- You must have a console connection to the switch, required when installing the RCF.
- You must have consulted the switch compatibility table on the [Cisco Ethernet switch page](#) for the supported ONTAP, NX-OS, and RCF versions.
- There can be command dependencies between the command syntax in the RCF and that found in versions of NX-OS.
- You must have referred to the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures on [Cisco Nexus 3000 Series Switches](#).
- You must have the current RCF.

## About this task

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

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



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

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

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



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

## Steps

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

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



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

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

```
set -privilege advanced
```

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

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

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
-----				
cluster1-02/cdp				
	e0a	cs1	Eth1/2	N3K-
C3232C				
	e0b	cs2	Eth1/2	N3K-
C3232C				
cluster1-01/cdp				
	e0a	cs1	Eth1/1	N3K-
C3232C				
	e0b	cs2	Eth1/1	N3K-
C3232C				

```
4 entries were displayed.
```

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

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

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

Node: cluster1-02

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

Node: cluster1-01

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

4 entries were displayed.

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

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

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

4 entries were displayed.

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

```

cluster1::*> **cluster ping-cluster -node cluster1-02**
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01      e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01      e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02      e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02      e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

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

```

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

```

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

4 entries were displayed.

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

```

system switch ethernet log enable-collection

```

```

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>

```



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

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

```
system cluster-switch log enable-collection
```

```

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>

```



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

## Install the NX-OS software

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

### Steps

1. Connect the cluster switch to the management network.



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

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

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

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

3. Copy the NX-OS software and EPLD images to the Nexus 3232C switch.

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

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

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

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

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

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and
unless
otherwise stated, there is no warranty, express or implied, including
but not
limited to warranties of merchantability and fitness for a particular
purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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

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

  Device name: cs2
  bootflash: 53298520 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 36 second(s)

  Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(3)
  Service:
```

```

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#

```

## 5. Install the NX-OS image.

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

```

cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

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

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

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

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

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

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

```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default

upgrade is not hitless

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-
Version	Upg-Required		
-----	-----	-----	-----
-----	-----	-----	-----

```

1          nxos          9.3(3)          9.3(4)
yes
1          bios          v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(01/28/2020)      no

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

Install is in progress, please wait.

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

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

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

Finishing the upgrade, switch will reboot in 10 seconds.
cs2#

```

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

```

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

```

```
GNU General Public License (GPL) version 3.0 or the GNU  
Lesser General Public License (LGPL) Version 2.1 or  
Lesser General Public License (LGPL) Version 2.0.  
A copy of each such license is available at  
http://www.opensource.org/licenses/gpl-2.0.php and  
http://opensource.org/licenses/gpl-3.0.html and  
http://www.opensource.org/licenses/lgpl-2.1.php and  
http://www.gnu.org/licenses/old-licenses/library.txt.
```

#### Software

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

#### Hardware

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

```
Device name: rtpnpi-mcc01-8200-ms-A1
```

```
bootflash: 53298520 kB
```

```
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)
```

```
Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
```

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

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

```
Service:
```

#### plugin

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

7. Upgrade the EPLD image and reboot the switch.

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

EPLD Device	Version
MI FPGA	0x12
IO FPGA	0x11

```
cs2# install epld bootflash:n9000-epld.9.3.4.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x12	0x12	No
1	SUP	IO FPGA	0x11	0x12	Yes

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

Module 1 EPLD upgrade is successful.

```
cs2#
```

8. After the switch reboot, log in again, upgrade the EPLD golden image and reboot the switch once again.

```

cs2# install epld bootflash:n9000-epld.9.3.4.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module          Type          Upgradable          Impact          Reason
-----
1              SUP              Yes              disruptive      Module Upgradable

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
cs2#

```

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

```

cs2# show version module 1 epld

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

```

## Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 3232C switch for the first time. You can also use this procedure to upgrade your RCF version.

### About this task

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

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



- The procedure requires the -se of both ONTAP commands and Cisco Nexus 3000 Series Switches commands; ONTAP commands are used unless otherwise indicated.
- Before you perform this procedure, make sure that you have a current backup of the switch configuration.

## Steps

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

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface          Platform
-----
cluster1-01/cdp
                e0a    cs1                      Ethernet1/7        N3K-
C3232C
                e0d    cs2                      Ethernet1/7        N3K-
C3232C
cluster1-02/cdp
                e0a    cs1                      Ethernet1/8        N3K-
C3232C
                e0d    cs2                      Ethernet1/8        N3K-
C3232C
cluster1-03/cdp
                e0a    cs1                      Ethernet1/1/1      N3K-
C3232C
                e0b    cs2                      Ethernet1/1/1      N3K-
C3232C
cluster1-04/cdp
                e0a    cs1                      Ethernet1/1/2      N3K-
C3232C
                e0b    cs2                      Ethernet1/1/2      N3K-
C3232C
cluster1::*>
```

2. Check the administrative and operational status of each cluster port.
  - a. Verify that all the cluster ports are up with a healthy status: `network port show -role cluster`



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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
8 entries were displayed.
```

```
Node: cluster1-03
```

```
Ignore
```

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

```
Node: cluster1-04
```

```

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

```

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

```

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

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                               Type                               Address                           Model
-----
cs1                                  cluster-network                   10.233.205.92
NX3232C
    Serial Number: FOXXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(4)
    Version Source: CDP

cs2                                  cluster-network                   10.233.205.93
NX3232C
    Serial Number: FOXXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(4)
    Version Source: CDP

2 entries were displayed.
```

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

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

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

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

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

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

```

cluster1::*> network interface show -role cluster

```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----				
Cluster				
e0a	true	cluster1-01_clus1 up/up	169.254.3.4/23	cluster1-01
e0a	false	cluster1-01_clus2 up/up	169.254.3.5/23	cluster1-01
e0a	true	cluster1-02_clus1 up/up	169.254.3.8/23	cluster1-02
e0a	false	cluster1-02_clus2 up/up	169.254.3.9/23	cluster1-02
e0a	true	cluster1-03_clus1 up/up	169.254.1.3/23	cluster1-03
e0a	false	cluster1-03_clus2 up/up	169.254.1.1/23	cluster1-03
e0a	true	cluster1-04_clus1 up/up	169.254.1.6/23	cluster1-04
e0a	false	cluster1-04_clus2 up/up	169.254.1.7/23	cluster1-04

```

8 entries were displayed.
cluster1::*>

```

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

```

cluster1::*> cluster show

```

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

```

4 entries were displayed.
cluster1::*>

```

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

```
show running-config
```

8. Clean the configuration on switch cs2 and perform a basic setup.
  - a. Clean the configuration. This step requires a console connection to the switch.

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

- b. Perform a basic setup of the switch.
9. Copy the RCF to the bootflash of switch cs2 using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 3000 Series NX-OS Command Reference](#) guides.

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

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

10. Apply the RCF previously downloaded to the bootflash.

For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 3000 Series NX-OS Command Reference](#) guides.

This example shows the RCF file `Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt` being installed on switch cs2:

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
```

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

```
cs2# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
```

```

* Switch      : Cisco Nexus 3232C
* Filename    : Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date       : Oct-20-2020
* Version    : v1.6
*
* Port Usage : Breakout configuration
* Ports 1- 3: Breakout mode (4x10GbE) Intra-Cluster Ports, int e1/1/1-4,
* e1/2/1-4, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25GbE) Intra-Cluster/HA Ports, int e1/4/1-4,
* e1/5/1-4, e1/6/1-4
* Ports 7-30: 40/100GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
* Ports 33-34: 10GbE Intra-Cluster 10GbE Ports, int e1/33-34
*
* IMPORTANT NOTES
* - Load Nexus_3232C_RCF_v1.6-Cluster-HA.txt for non breakout config
*
* - This RCF utilizes QoS and requires TCAM re-configuration, requiring RCF
*   to be loaded twice with the Cluster Switch rebooted in between.
*
* - Perform the following 4 steps to ensure proper RCF installation:
*
*   (1) Apply RCF first time, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on ports...
*       - TCAM region is not configured for feature QoS class IPv4 ingress...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect following messages:
*       - % Invalid command at '^' marker
*       - Syntax error while parsing...
*
*   (4) Save running-configuration again
*****

```



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

1. 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.

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

For more information on Cisco commands, see the appropriate guide in the [Cisco Nexus 3000 Series NX-OS Command Reference](#) guides.

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

3. Reboot switch cs2. You can ignore the "cluster ports down" events reported on the nodes while the switch reboots.

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

4. Apply the same RCF and save the running configuration for a second time.

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
cs2# copy running-config startup-config
[#####] 100% Copy complete
```

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

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

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

Node: cluster1-01

Ignore

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

```

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

Node: cluster1-02

Ignore

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

Node: cluster1-03

Ignore

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

Node: cluster1-04

Ignore

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

```



```

healthy false
e0d          Cluster          Cluster          up    9000    auto/100000
healthy false
8 entries were displayed.

```

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

```

cluster1::*> network device-discovery show -protocol cdp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
              e0a    cs1                      Ethernet1/7      N3K-
C3232C
              e0d    cs2                      Ethernet1/7      N3K-
C3232C
cluster01-2/cdp
              e0a    cs1                      Ethernet1/8      N3K-
C3232C
              e0d    cs2                      Ethernet1/8      N3K-
C3232C
cluster01-3/cdp
              e0a    cs1                      Ethernet1/1/1    N3K-
C3232C
              e0b    cs2                      Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
              e0a    cs1                      Ethernet1/1/2    N3K-
C3232C
              e0b    cs2                      Ethernet1/1/2    N3K-
C3232C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type                      Address              Model
-----
cs1                          cluster-network          10.233.205.90        N3K-
C3232C
    Serial Number: FOXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version

```

```

          9.3(4)
Version Source: CDP

cs2                cluster-network    10.233.205.91    N3K-
C3232C
  Serial Number: FOXXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
          9.3(4)
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.

```

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

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

```

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

```

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

```

cluster1::*> network interface show -role cluster

```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	
Port	Home				
-----					
Cluster					
e0d	false	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	true	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	false	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	true	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0b	false	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	false	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

```

8 entries were displayed.
cluster1::*>

```

8. Verify that the cluster is healthy: cluster show

```

cluster1::*> cluster show

```

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

```

4 entries were displayed.
cluster1::*>

```

9. Repeat Steps 7 to 14 on switch cs1.

10. Enable auto-revert on the cluster LIFs.

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

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

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

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

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

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

```

cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
-----
-----
Group Port-          Type      Protocol  Member Ports
      Channel
-----
-----
1      Pol (SU)      Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
cs1#

```

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

```

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

```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----				
Cluster				
e0d	cluster1-01_clus1	up/up	169.254.3.4/23	cluster1-01
e0d	cluster1-01_clus2	up/up	169.254.3.5/23	cluster1-01
e0d	cluster1-02_clus1	up/up	169.254.3.8/23	cluster1-02
e0d	cluster1-02_clus2	up/up	169.254.3.9/23	cluster1-02
e0b	cluster1-03_clus1	up/up	169.254.1.3/23	cluster1-03
e0b	cluster1-03_clus2	up/up	169.254.1.1/23	cluster1-03
e0b	cluster1-04_clus1	up/up	169.254.1.6/23	cluster1-04
e0b	cluster1-04_clus2	up/up	169.254.1.7/23	cluster1-04

```

8 entries were displayed.
cluster1::*>

```

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

```

cluster1::*> cluster show

```

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

```

4 entries were displayed.
cluster1::*>

```

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

```

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

```

## Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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.