



Configure software

Install and maintain

NetApp
February 20, 2026

Table of Contents

- Configure software 1
 - Software install workflow for Cisco Nexus 3132Q-V cluster switches 1
 - Configure the Cisco Nexus 3132Q-V switch 1
 - Prepare to install NX-OS software and Reference Configuration File 4
 - Install the NX-OS software 10
 - Review requirements 10
 - Install the software 10
 - Install or upgrade the RCF 27
 - Install or upgrade the Reference Configuration File (RCF) overview 27
 - Install the Reference Configuration File (RCF) 29
 - Upgrade your Reference Configuration File (RCF) 40
- Verify your SSH configuration 61
- Reset the 3132Q-V cluster switch to factory defaults 62

Configure software

Software install workflow for Cisco Nexus 3132Q-V cluster switches

To install and configure the software for a Cisco Nexus 3132Q-V switch and install or upgrade the Reference Configuration File (RCF), follow these steps:

1

Configure the switch

Configure the 3132Q-V cluster switch.

2

Prepare to install the NX-OS software and RCF

The Cisco NX-OS software and RCF must be installed on Cisco 3132Q-V cluster switches.

3

Install or upgrade the NX-OS software

Download and install or upgrade the NX-OS software on the Cisco 3132Q-V cluster switch.

4

Install or upgrade the RCF

Install or upgrade the RCF after setting up the Cisco 3132Q-V switch.

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 3132Q-V cluster switch settings.

Configure the Cisco Nexus 3132Q-V switch

Follow this procedure to configure the Cisco Nexus 3132Q-V switch.

Before you begin

- Access to an HTTP, FTP or TFTP server at the installation site to download the applicable NX-OS and reference configuration file (RCF) releases.
- Applicable NX-OS version, downloaded from the [Cisco software download](#) page.
- Required network switch documentation, controller documentation, and ONTAP documentation. For more information, see [Required documentation](#).
- Applicable licenses, network and configuration information, and cables.

- Completed cabling worksheets. See [Complete Cisco Nexus 3132Q-V cabling worksheet](#).
- Applicable NetApp cluster network and management network RCFs, downloaded from the NetApp Support Site at mysupport.netapp.com for the switches that you receive. 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.

Steps

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

If you are installing your...	Then...
Cisco Nexus 3132Q-V in a NetApp system cabinet	See the <i>Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet</i> guide for instructions to install the switch in a NetApp cabinet.
Equipment in a Telco rack	See the procedures provided in the switch hardware installation guides and the NetApp installation and setup instructions.

2. Cable the cluster network and management network switches to the controllers using the completed cabling worksheet, as described in [Complete Cisco Nexus 3132Q-V cabling worksheet](#).
3. Power on the cluster network and management network switches and controllers.
4. Perform an initial configuration of the cluster network switches.

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

Prompt	Response
Abort Auto Provisioning and continue with normal setup? (yes/no)	Respond with yes . The default is no.
Do you want to enforce secure password standard? (yes/no)	Respond with yes . The default is yes.
Enter the password for admin:	The default password is "admin"; you must create a new, strong password. A weak password can be rejected.
Would you like to enter the basic configuration dialog? (yes/no)	Respond with yes at the initial configuration of the switch.
Create another login account? (yes/no)	Your answer depends on your site's policies on alternate administrators. The default is no .
Configure read-only SNMP community string? (yes/no)	Respond with no . The default is no.

Prompt	Response
Configure read-write SNMP community string? (yes/no)	Respond with no . The default is no.
Enter the switch name.	The switch name is limited to 63 alphanumeric characters.
Continue with Out-of-band (mgmt0) management configuration? (yes/no)	Respond with yes (the default) at that prompt. At the mgmt0 IPv4 address: prompt, enter your IP address: ip_address.
Configure the default-gateway? (yes/no)	Respond with yes . At the IPv4 address of the default-gateway: prompt, enter your default_gateway.
Configure advanced IP options? (yes/no)	Respond with no . The default is no.
Enable the telnet service? (yes/no)	Respond with no . The default is no.
Enabled SSH service? (yes/no)	Respond with yes . The default is yes. <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">  SSH is recommended when using Ethernet Switch Health Monitor (CSHM) for its log collection features. SSHv2 is also recommended for enhanced security. </div>
Enter the type of SSH key you want to generate (dsa/rsa/rsa1).	The default is rsa .
Enter the number of key bits (1024-2048).	Enter the key bits from 1024-2048.
Configure the NTP server? (yes/no)	Respond with no . The default is no.
Configure default interface layer (L3/L2):	Respond with L2 . The default is L2.
Configure default switch port interface state (shut/noshut):	Respond with noshut . The default is noshut.
Configure CoPP system profile (strict/moderate/lenient/dense):	Respond with strict . The default is strict.

Prompt	Response
Would you like to edit the configuration? (yes/no)	You should see the new configuration at this point. Review and make any necessary changes to the configuration you just entered. Respond with no at the prompt if you are satisfied with the configuration. Respond with yes if you want to edit your configuration settings.
Use this configuration and save it? (yes/no)	<p>Respond with yes to save the configuration. This automatically updates the kickstart and system images.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  If you do not save the configuration at this stage, none of the changes will be in effect the next time you reboot the switch. </div>

5. Verify the configuration choices you made in the display that appears at the end of the setup, and make sure that you save the configuration.
6. Check the version on the 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 [prepare to install the NX-OS and RCF](#).

Prepare to install NX-OS software and Reference Configuration File

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 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. See [What additional information do I need to install my equipment that is not in HWU?](#) for more information about switch installation requirements.



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.

About this task

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

Steps

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

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

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



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

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

```
set -privilege advanced
```

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

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

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

Show example

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
-----	-----	-----	-----	
cluster1-02/cdp				
	e0a	cs1	Eth1/2	N3K-
C3132Q-V				
	e0b	cs2	Eth1/2	N3K-
C3132Q-V				
cluster1-01/cdp				
	e0a	cs1	Eth1/1	N3K-
C3132Q-V				
	e0b	cs2	Eth1/1	N3K-
C3132Q-V				

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

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

Node: cluster1-01

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

b. Display information about the LIFs:

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

Show example

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

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

5. Verify the connectivity of the remote cluster interfaces:

ONTAP 9.9.1 and later

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

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

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

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

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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)

```

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

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

Show example

```

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

```

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

What's next?

After you've prepared to install the NX-OS software and RCF, you [install the NX-OS software](#).

Install the NX-OS software

Follow this procedure to install the NX-OS software on the Nexus 3132Q-V cluster switch.

Review requirements

Before you begin

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

Suggested documentation

- [Cisco Ethernet switch](#). Consult the switch compatibility table for the supported ONTAP and NX-OS versions.
- [Cisco Nexus 3000 Series Switches](#). Consult the appropriate software and upgrade guides available on the Cisco web site for complete documentation on the Cisco switch upgrade and downgrade procedures.

Install the software

About this task

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

Be sure to complete the procedure in [Prepare to install NX-OS software and Reference Configuration File](#), and then follow the steps below.

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

```
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                      Ethernet1/7      N3K-
C3132Q-V
              e0d    cs2                      Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
              e0a    cs1                      Ethernet1/8      N3K-
C3132Q-V
              e0d    cs2                      Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
              e0a    cs1                      Ethernet1/1/1    N3K-
C3132Q-V
              e0b    cs2                      Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
              e0a    cs1                      Ethernet1/1/2    N3K-
C3132Q-V
              e0b    cs2                      Ethernet1/1/2    N3K-
C3132Q-V
cluster1::*>
```

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

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

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

Show example

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

Node: cluster1-01

Ignore

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

Node: cluster1-02

Ignore

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

Node: cluster1-03

Ignore

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

```
Node: cluster1-04
```

```
Ignore
```

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

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

```
network interface show -role Cluster
```

Show example

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

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

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

Show example

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
cs1                                         cluster-network    10.233.205.90
N3K-C3132Q-V
  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
N3K-C3132Q-V
  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 to the Nexus 3132Q-V switch using one of the following transfer protocols: FTP, TFTP, SFTP, or SCP. For more information on Cisco commands, see the appropriate guide in [Cisco Nexus 3000 Series NX-OS Command Reference guides](#).

Show example

```
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: xxxxxxxx
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.
```

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

```
show version
```

Show example

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

Software
  BIOS: version 04.25
  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 Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxxx23

  Device name: cs2
  bootflash: 15137792 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
Reason: Reset Requested by CLI command reload
System version: 9.3(3)
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.9.3.4.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      v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(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#
```

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 04.25
  NXOS: version 9.3(4)
  BIOS compile time: 05/22/2019
  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 Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxxx23

  Device name: cs2
  bootflash: 15137792 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
Reason: Reset Requested by CLI command reload
System version: 9.3(4)
Service:

plugin
Core Plugin, Ethernet Plugin

Active Package(s) :

cs2#
```

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

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

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

Show example

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

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

```
Node: cluster1-04

Ignore

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

b. Verify the switch health from the cluster.

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

Show example

```
cluster1::*> network device-discovery show -protocol cdp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                        Ethernet1/7
N3K-C3132Q-V
          e0d    cs2                        Ethernet1/7
N3K-C3132Q-V
cluster01-2/cdp
          e0a    cs1                        Ethernet1/8
N3K-C3132Q-V
          e0d    cs2                        Ethernet1/8
N3K-C3132Q-V
cluster01-3/cdp
          e0a    cs1                        Ethernet1/1/1
N3K-C3132Q-V
          e0b    cs2                        Ethernet1/1/1
N3K-C3132Q-V
cluster1-04/cdp
          e0a    cs1                        Ethernet1/1/2
N3K-C3132Q-V
          e0b    cs2                        Ethernet1/1/2
N3K-C3132Q-V

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                Type                Address
Model
-----
-----
cs1                    cluster-network    10.233.205.90
N3K-C3132Q-V
  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
```

```

N3K-C3132Q-V
  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.

```

11. 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::*>

```

12. Repeat steps 6 to 11 on switch cs1.

13. Enable auto-revert on the cluster LIFs.

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

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

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

Show example

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

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

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

What's next?

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

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 3132Q-V

switches 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.

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 two ONTAP clusters with at least eight nodes, including nodes that use shared Cluster+HA ports.
4-Cluster-HA-Breakout	Supports four ONTAP 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/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 3132Q-V switches. Choose the applicable RCF version for your configuration. See [Cisco Ethernet Switches](#) for more information.

RCF name
Cluster-HA-Breakout RCF v1.xx
Cluster-HA RCF v1.xx

RCF name
Cluster RCF 1.xx

Suggested documentation

- [Cisco Ethernet Switches \(NSS\)](#)

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 3000 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 **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 examples in this procedure use four 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.

For details of the available RCF configurations, see [Software install workflow](#).

Commands used

The procedure requires the use of both ONTAP commands and Cisco Nexus 3000 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 [install the RCF](#) or [upgrade your RCF](#) as required.

Install the Reference Configuration File (RCF)

You install the Reference Configuration File (RCF) after setting up the Nexus 3132Q-V switches for the first time.

Before you begin

Verify the following installations and connections:

- A current backup of the switch configuration.

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

About this task

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

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 enable 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.

Step 1: Install the RCF on the switches

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

```
network device-discovery show
```

Show example

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
              e0a    cs1                      Ethernet1/7      N3K-
C3132Q-V
              e0d    cs2                      Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
              e0a    cs1                      Ethernet1/8      N3K-
C3132Q-V
              e0d    cs2                      Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
              e0a    cs1                      Ethernet1/1/1    N3K-
C3132Q-V
              e0b    cs2                      Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
              e0a    cs1                      Ethernet1/1/2    N3K-
C3132Q-V
              e0b    cs2                      Ethernet1/1/2    N3K-
C3132Q-V
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 -ipSpace Cluster
```

Show example

```
cluster1::*> network port show -ipSpace Cluster
Node: cluster1-01

Ignore

Health Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status
-----
-----
Speed (Mbps)
e0a Cluster Cluster up 9000 auto/100000
healthy false
e0d Cluster Cluster up 9000 auto/100000
healthy false
Node: cluster1-02

Ignore

Health Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status
-----
-----
Speed (Mbps)
e0a Cluster Cluster up 9000 auto/100000
healthy false
e0d Cluster Cluster up 9000 auto/100000
healthy false
8 entries were displayed.
Node: cluster1-03

Ignore

Health Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status Status
-----
-----
Speed (Mbps)
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           Admin/Oper Address/Mask      Node
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 e0d      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 e0d      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
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                    10.0.0.1
NX3132QV
  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                    10.0.0.2
NX3132QV
  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.
```



For ONTAP 9.8 and later, use the command `system switch ethernet show -is-monitoring-enabled-operational true`.

3. Disable auto-revert on the cluster LIFs.

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

Make sure that auto-revert is disabled after running this command.

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

```

cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit

```



The number of ports displayed varies based on the number of nodes in the cluster.

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

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

Show example

```

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	169.254.3.4/23	
cluster1-01	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0a	false		
	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	e0a	false		
	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	e0a	false		
	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	e0a	false		

```

cluster1::*>

```

- 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
cluster1::*>
```

7. 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
```

8. Record any custom additions between the current running-config and the RCF file in use.



Make sure to configure the following: * Username and password * Management IP address * Default gateway * Switch name

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



When upgrading or applying a new RCF, you must erase the switch settings and perform basic configuration. You must be connected to the switch serial console port to set up the switch again.

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

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

```
cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region racl 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region e-racl 256" >>
```

```
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region qos 256" >>  
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.

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

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

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

```
cs2# write erase
```

```
Warning: This command will erase the startup-configuration.
```

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

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

```
cs2# copy bootflash:write_erase.cfg startup-config
```

14. Reboot the switch:

```
cs2# reload
```

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

15. Repeat Steps 7 to 14 on switch cs1.

16. 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 | grep up
```

Show example

```
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) --
.
.
```

2. Verify that the ISL between cs1 and cs2 is functional:

```
show port-channel summary
```

Show example

```
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      Po1 (SU)        Eth       LACP      Eth1/31 (P)  Eth1/32 (P)
cs1#
```

3. 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 cluster1-01_clus1 up/up      169.254.3.4/23
          e0d             true
cluster1-01 cluster1-01_clus2 up/up      169.254.3.5/23
          e0d             true
cluster1-02 cluster1-02_clus1 up/up      169.254.3.8/23
          e0d             true
cluster1-02 cluster1-02_clus2 up/up      169.254.3.9/23
          e0d             true
cluster1-03 cluster1-03_clus1 up/up      169.254.1.3/23
          e0b             true
cluster1-03 cluster1-03_clus2 up/up      169.254.1.1/23
          e0b             true
cluster1-04 cluster1-04_clus1 up/up      169.254.1.6/23
          e0b             true
cluster1-04 cluster1-04_clus2 up/up      169.254.1.7/23
          e0b             true
cluster1::*>
```

4. 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
cluster1::*>
```

Step 3: Setup your ONTAP cluster

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

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

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

What's next?

After you've installed the RCF, you can [verify the SSH configuration](#).

Upgrade your Reference Configuration File (RCF)

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

Before you begin

Make sure you have the following:

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

If you need to change the boot configuration to reflect the current boot images, you must do so before reapplying the RCF so that the correct version is 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 prior to erasing the switch settings.

Step 1: Prepare for the upgrade

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

```
network device-discovery show
```

Show example

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
              e0a    cs1                      Ethernet1/7      N3K-
C3132Q-V
              e0d    cs2                      Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
              e0a    cs1                      Ethernet1/8      N3K-
C3132Q-V
              e0d    cs2                      Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
              e0a    cs1                      Ethernet1/1/1    N3K-
C3132Q-V
              e0b    cs2                      Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
              e0a    cs1                      Ethernet1/1/2    N3K-
C3132Q-V
              e0b    cs2                      Ethernet1/1/2    N3K-
C3132Q-V
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 -ipSpace Cluster
```

Show example

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

Node: cluster1-01

Ignore

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

Node: cluster1-02

Ignore

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

Node: cluster1-03

Ignore

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

```
Node: cluster1-04
```

```
Ignore
```

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

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

```
network interface show -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  cluster1-01_clus1  up/up      169.254.3.4/23
            e0a      true
cluster1-01  cluster1-01_clus2  up/up      169.254.3.5/23
            e0d      true
cluster1-02  cluster1-02_clus1  up/up      169.254.3.8/23
            e0a      true
cluster1-02  cluster1-02_clus2  up/up      169.254.3.9/23
            e0d      true
cluster1-03  cluster1-03_clus1  up/up      169.254.1.3/23
            e0a      true
cluster1-03  cluster1-03_clus2  up/up      169.254.1.1/23
            e0b      true
cluster1-04  cluster1-04_clus1  up/up      169.254.1.6/23
            e0a      true
cluster1-04  cluster1-04_clus2  up/up      169.254.1.7/23
            e0b      true
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    10.0.0.1
NX3132QV
  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    10.0.0.2
NX3132QV
  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.
```



For ONTAP 9.8 and later, use the command `system switch ethernet show -is-monitoring-enabled-operational true`.

3. Disable auto-revert on the cluster LIFs.

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

Make sure that auto-revert is disabled after running this command.

Step 2: Configure ports

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

```

cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit

```



The number of ports displayed varies based on the number of nodes in the cluster.

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

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

Show example

```

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	169.254.3.4/23	
cluster1-01	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0a	false		
	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	e0a	false		
	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	e0a	false		
	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	e0a	false		

```

cluster1::*>

```

3. 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
cluster1::*>
```

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
```

5. Record any custom additions between the current running-config and the RCF file in use.

Make sure to configure the following:



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

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



When upgrading or applying a new RCF, you must erase the switch settings and perform basic configuration.

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

7. When upgrading to RCF version 1.12 and later, run the following commands:

```
cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region racl 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region e-racl 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region qos 256" >>
bootflash:write_erase.cfg
```

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

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

- Issue the `write erase` command to erase the current saved configuration:

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

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

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

```
cs2# copy bootflash:write_erase.cfg startup-config
```

- Reboot the switch:

```
cs2# reload
```

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

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

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

- 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.

Show example

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3132QV_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)...
```

14. 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.

Show example

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands
```



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

15. 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.



For steps on how to bring your 10GbE ports online after an upgrade of the RCF, see the Knowledge Base article [10GbE ports on a Cisco 3132Q cluster switch do not come online](#).

16. 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.

Show example

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

17. Reboot switch cs2. You can ignore both the "cluster ports down" events reported on the nodes while the switch reboots and the error `% Invalid command at '^' marker` output.

```
cs2# reload
```

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

18. Reapply any previous customizations to the switch configuration. Refer to [Review cabling and configuration considerations](#) for details of any further changes required.
19. 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					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-04
```

```
Ignore
```

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

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
N3K-C3132Q-V
          e0d    cs2                        Ethernet1/7
N3K-C3132Q-V
cluster01-2/cdp
          e0a    cs1                        Ethernet1/8
N3K-C3132Q-V
          e0d    cs2                        Ethernet1/8
N3K-C3132Q-V
cluster01-3/cdp
          e0a    cs1                        Ethernet1/1/1
N3K-C3132Q-V
          e0b    cs2                        Ethernet1/1/1
N3K-C3132Q-V
cluster1-04/cdp
          e0a    cs1                        Ethernet1/1/2
N3K-C3132Q-V
          e0b    cs2                        Ethernet1/1/2
N3K-C3132Q-V

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                               Type                Address
Model
-----
-----
cs1                                   cluster-network     10.233.205.90
N3K-C3132Q-V
  Serial Number: FOXXXXXXXXGD
  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-C3132Q-V
  Serial Number: FOXXXXXXXXGS
    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.

```



For ONTAP 9.8 and later, use the command `system switch ethernet show -is -monitoring-enabled-operational true`.

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.

```



It can take up to 5 minutes for the cluster nodes to report as healthy.

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

Show example

```

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# exit

```



The number of ports displayed varies based on the number of nodes in the cluster.

21. Verify that the cluster LIFs have migrated to the ports hosted on switch cs2. This might take a few seconds.

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

Show example

```
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	169.254.3.4/23	
cluster1-01	e0d	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	false		
	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	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
cluster1::*>
```

22. 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::*>
```

23. Repeat Steps 1 to 19 on switch cs1.
24. Enable auto-revert on the cluster LIFs.

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

25. 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
```

Step 3: Verify the configuration

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

```
show interface brief | grep up
```

Show example

```
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) --
.
.
```

2. Verify that the ISL between cs1 and cs2 is functional:

```
show port-channel summary
```

Show example

```
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      Po1(SU)        Eth       LACP      Eth1/31(P)  Eth1/32(P)
cs1#
```

3. Verify that the cluster LIFs have reverted to their home ports:

```
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 cluster1-01_clus1 up/up      169.254.3.4/23
          e0d             true
cluster1-01 cluster1-01_clus2 up/up      169.254.3.5/23
          e0d             true
cluster1-02 cluster1-02_clus1 up/up      169.254.3.8/23
          e0d             true
cluster1-02 cluster1-02_clus2 up/up      169.254.3.9/23
          e0d             true
cluster1-03 cluster1-03_clus1 up/up      169.254.1.3/23
          e0b             true
cluster1-03 cluster1-03_clus2 up/up      169.254.1.1/23
          e0b             true
cluster1-04 cluster1-04_clus1 up/up      169.254.1.6/23
          e0b             true
cluster1-04 cluster1-04_clus2 up/up      169.254.1.7/23
          e0b             true
cluster1::*>
```

4. 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
cluster1::*>
```

5. Verify the connectivity of the remote cluster interfaces:

ONTAP 9.9.1 and later

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

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

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

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

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

Packet	Source	Destination
Node	LIF	LIF
Date		
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)

```

What's next?

After you've upgraded your RCF, you [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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
l7nwlIoc6HBejxluIObAH8hrW8kR+gj0ZAFpPNeLGTg3APj/yIPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDsrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRALZeHwQ

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



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

What's next?

After you've verified your SSH configuration, you can [configure switch health monitoring](#).

Reset the 3132Q-V cluster switch to factory defaults

To reset the 3132Q-V cluster switch to factory defaults, you must erase the 3132Q-V

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 resetting the switch, you can [reconfigure](#) it according to your requirements.

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.