# NetApp

# Configure software

## Cluster and storage switches

NetApp
April 25, 2024

# Table of Contents

# Configure software

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

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

**What you'll need**

- A fully functioning cluster (no errors in the logs or similar issues).
- Appropriate software and upgrade guides, which are available from Cisco Nexus 9000 Series Switches.

**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.

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

- The names of the two Cisco switches are `cs1` and `cs2`.
- The node names are `node1` and `node2`.
- The cluster LIF names are `node1_clus1` and `node1_clus2` for node1 and `node2_clus1` and `node2_clus2` for node2.
- The `cluster1::*>` prompt indicates the name of the cluster.

**About this task**

The procedure requires the use of both ONTAP commands and Cisco Nexus 9000 Series Switches commands; ONTAP commands are used unless otherwise indicated. The command outputs might vary depending on different releases of ONTAP.

**Steps**

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

   ```
   set -privilege advanced
   ```

   The advanced prompt (`*>`) appears.

2. 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.

   The following command suppresses automatic case creation for two hours:

```
cluster1:> **system node autosupport invoke -node * -type all -message
MAINT=2h**
```

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/       Local  Discovered
 Protocol    Port   Device (LLDP: ChassisID)  Interface
 Platform
 ----------- ------ ------------------------- ----------------
 ----------------
 node2       /cdp
             e0a    cs1                        Eth1/2          N9K-
 C92300YC
             e0b    cs2                        Eth1/2          N9K-
 C92300YC
 node1       /cdp
             e0a    cs1                        Eth1/1          N9K-
 C92300YC
             e0b    cs2                        Eth1/1          N9K-
 C92300YC

 4 entries were displayed.
```

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

   a. Display the network port attributes: `network port show –ipspace Cluster`

**Show example**

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

Node: node2
                                            Speed(Mbps)
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: node1
                                            Speed(Mbps)
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

4 entries were displayed.
```

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

**Show example**

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


            Logical     Status     Network                Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask           Node
Port     Home
----------- ---------- ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1  up/up     169.254.209.69/16  node1
e0a      true
            node1_clus2  up/up     169.254.49.125/16  node1
e0b      true
            node2_clus1  up/up     169.254.47.194/16  node2
e0a      true
            node2_clus2  up/up     169.254.19.183/16  node2
e0b      true

4 entries were displayed.
```

5. Ping the remote cluster LIFs:

```
cluster ping-cluster -node node-name
```

**Show example**

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

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

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

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

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

**Show example**

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

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

7. For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files using the commands:

`system cluster-switch log setup-password` and `system cluster-switch log enable-collection`

**Show example**

```
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.

**What's next?**
Install the NX-OS software.

# Install the NX-OS software

Follow this procedure to install the NX-OS software on the Nexus 92300YC switch.

NX-OS is a network operating system for the Nexus series of Ethernet switches and MDS series of Fibre Channel (FC) storage area network switches provided by Cisco Systems.

## Review requirements

### Supported ports and node connections

- The Inter-Switch Links (ISLs) supported for the Nexus 92300YC switches are ports 1/65 and 1/66.
- The node connections supported for the Nexus 92300YC switches are ports 1/1 through 1/66.

### What you'll need

- Applicable NetApp Cisco NX-OS software for your switches from the NetApp Support Site, available from mysupport.netapp.com
- A fully functioning cluster (no errors in the logs or similar issues).
- Cisco Ethernet switch page. Consult the switch compatibility table for the supported ONTAP and NX-OS versions.

## Install the software

The examples in this procedure use two nodes, but you can have up to 24 nodes in a cluster.

### About the examples

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

- The Nexus 92300YC switch names are `cs1` and `cs2`.
- The example used in this procedure starts the upgrade on the second switch, *cs2*.
- The cluster LIF names are `node1_clus1` and `node1_clus2` for node1, and `node2_clus1` and `node2_clus2` for node2.
- The IPspace name is `Cluster`.
- The `cluster1::*>` prompt indicates the name of the cluster.
- The cluster ports on each node are named `e0a` and `e0b`.

    See the *Hardware Universe^* for the actual cluster ports supported on your platform.

### Steps

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

**Show example**

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

```
cs2# ping 172.19.2.1
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 92300YC switch.

**Show example**

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.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.9.2.2.bin  /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.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.9.2.2.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.9.2.2.img  /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.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:

```
show version
```

**Show example**

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.31
  NXOS: version 9.2(1)
  BIOS compile time:  05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time:  7/17/2018 16:00:00 [07/18/2018 00:21:19]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
  System version: 9.2(1)
  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.

**Show example**

```
cs2# install all nxos bootflash:nxos.9.2.2.bin

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

Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.2.2.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                             9.2(1)
9.2(2)        yes
  1       bios    v05.31(05/17/2018):v05.28(01/18/2018)
v05.33(09/08/2018)        yes
```

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


Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading
bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[] 100% -- SUCCESS
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully deactivated virtual service 'guestshell+'

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

6. 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) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.33
  NXOS: version 9.2(2)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.2.2.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)

Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```

```
   Reason: Reset due to upgrade
   System version: 9.2(1)
   Service:

plugin
   Core Plugin, Ethernet Plugin

Active Package(s):
```

7. Upgrade the EPLD image and reboot the switch.

**Show example**

```
cs2# show version module 1 epld

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

cs2# install epld bootflash:n9000-epld.9.2.2.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                  0x07           0x07
No
   1    SUP   IO FPGA                  0x17           0x19
Yes
   1    SUP   MI FPGA2                 0x02           0x02
No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y


Proceeding to upgrade Modules.


Starting Module 1 EPLD Upgrade


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

```
        1          SUP           Success


EPLDs upgraded.


Module 1 EPLD upgrade is successful.
```

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

**Show example**

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

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

**What's next?**

Install the Reference Configuration File

# Install the Reference Configuration File (RCF)

You can install the RCF after setting up the Nexus 92300YC 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 `node1` and `node2`.

- The cluster LIF names are `node1_clus1`, `node1_clus2`, `node2_clus1`, and `node2_clus2`.

- The `cluster1::*>` prompt indicates the name of the cluster.

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

- Before you perform this procedure, make sure that you have a current backup of the switch configuration.

- 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.

**Steps**

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
----------- ------ ------------------------ ----------------
------------
node1/cdp
            e0a     cs1                          Ethernet1/1/1     N9K-
C92300YC
            e0b     cs2                          Ethernet1/1/1     N9K-
C92300YC
node2/cdp
            e0a     cs1                          Ethernet1/1/2     N9K-
C92300YC
            e0b     cs2                          Ethernet1/1/2     N9K-
C92300YC
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: node1

Ignore
                                                 Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status    Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000 auto/100000
healthy false
e0d       Cluster      Cluster          up   9000 auto/100000
healthy false

Node: node2

Ignore
                                                 Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status    Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000 auto/100000
healthy false
e0d       Cluster      Cluster          up   9000 auto/100000
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
          node1_clus1          up/up      169.254.3.4/23    node1
e0c      true
          node1_clus2          up/up      169.254.3.5/23    node1
e0d      true
          node2_clus1          up/up      169.254.3.8/23    node2
e0c      true
          node2_clus2          up/up      169.254.3.9/23    node2
e0d      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    10.233.205.92
N9K-C92300YC
        Serial Number: FOXXXXXXXGS
          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
N9K-C92300YC
        Serial Number: FOXXXXXXXGD
          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 e1/1-64
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 -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
            node1_clus1        up/up        169.254.3.4/23     node1
e0c     true
            node1_clus2        up/up        169.254.3.5/23     node1
e0c     false
            node2_clus1        up/up        169.254.3.8/23     node2
e0c     true
            node2_clus2        up/up        169.254.3.9/23     node2
e0c     false
cluster1::*>
```

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

**Show example**

```
cluster1::*> *cluster show*
Node           Health  Eligibility   Epsilon
-------------- ------- ------------ -------
node1          true    true          false
node2          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. Clean the configuration on switch cs2 and perform a basic setup.

> ⚠️ When updating 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.

   a. Clean the configuration:

**Show example**

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

b. Perform a reboot of the switch:

**Show example**

```
(cs2)# reload

Are you sure you would like to reset the system? (y/n) y
```

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 9000 Series Switches 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: /code/Nexus_92300YC_RCF_v1.0.2.txt
Enter hostname for the tftp 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:
tftp> progress
Progress meter enabled
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin
/code/Nexus_92300YC_R  100% 9687   530.2KB/s   00:00
tftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

10. Apply the RCF previously downloaded to the bootflash.

For more information on Cisco commands, see the appropriate guide in the Cisco Nexus 9000 Series Switches guides.

This example shows the RCF file `Nexus_92300YC_RCF_v1.0.2.txt` being installed on switch cs2:

```
cs2# copy Nexus_92300YC_RCF_v1.0.2.txt running-config echo-commands


Disabling ssh: as its enabled right now:
 generating ecdsa key(521 bits)......
generated ecdsa key

Enabling ssh: as it has been disabled
 this command enables edge port type (portfast) by default on all
interfaces. You
 should now disable edge port type (portfast) explicitly on switched
ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.

Edge port type (portfast) should only be enabled on ports connected to a
single
 host. Connecting hubs, concentrators, switches, bridges, etc...  to
this
 interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
 Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet1/1 but will
only
 have effect when the interface is in a non-trunking mode.

...

Copy complete, now saving to disk (please wait)...
Copy complete.
```

11. Verify on the switch that the RCF has been merged successfully:

   show running-config

```
cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019

version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJ1RtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #


*

*

*   Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)

*

*

*

*   Ports 1/1  - 1/48: 10GbE Intra-Cluster Node Ports

*

*   Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports

*

*   Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports

*

*

*
```

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

12.  Verify that the RCF file is the correct newer version: `show running-config`

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

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

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

13. 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 9000 Series Switches guides.

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

14. 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
    ```

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

    a. Verify that e0d 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: node1

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: node2

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
```

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

**Show example**

```
cluster1::*> *network device-discovery show -protocol cdp*
Node/        Local  Discovered
Protocol     Port   Device (LLDP: ChassisID)  Interface
Platform
-----------  ------ ------------------------  -----------------
------------
node1/cdp
             e0a    cs1                        Ethernet1/1
N9K-C92300YC
             e0b    cs2                        Ethernet1/1
N9K-C92300YC
node2/cdp
             e0a    cs1                        Ethernet1/2
N9K-C92300YC
             e0b    cs2                        Ethernet1/2
N9K-C92300YC

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                          Type              Address
Model
--------------------------  ----------------- -----------------
------------
cs1                             cluster-network   10.233.205.90
N9K-C92300YC
     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
N9K-C92300YC
     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.
```

```
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.
```

16. 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 e1/1-64
cs1(config-if-range)# shutdown
```

17. 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*
           Logical          Status     Network                   Current
Current Is
Vserver     Interface        Admin/Oper Address/Mask          Node
Port    Home
----------- ---------------- ---------- ------------------
---------------- ------- ----
Cluster
            node1_clus1      up/up      169.254.3.4/23        node1
e0d     false
            node1_clus2      up/up      169.254.3.5/23        node1
e0d     true
            node2_clus1      up/up      169.254.3.8/23        node2
e0d     false
            node2_clus2      up/up      169.254.3.9/23        node2
e0d     true
cluster1::*>
```

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

**Show example**

```
cluster1::*> *cluster show*
Node            Health   Eligibility   Epsilon
--------------  -------- ------------- -------
node1           true     true          false
node2           true     true          false
cluster1::*>
```

19. Repeat Steps 7 to 14 on switch cs1.

20. Enable auto-revert on the cluster LIFs.

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

21. 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
```

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

```
cs1# show interface brief | grep up
.
.
Ethernet1/1     1        eth  access up      none
10G(D) --
Ethernet1/2     1        eth  access up      none
10G(D) --
Ethernet1/3     1        eth  trunk  up      none
100G(D) --
Ethernet1/4     1        eth  trunk  up      none
100G(D) --
.
.
```

23. 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      Eth1/65(P)   Eth1/66(P)
cs1#
```

24. 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
          node1_clus1   up/up      169.254.3.4/23     node1
e0d     true
          node1_clus2   up/up      169.254.3.5/23     node1
e0d     true
          node2_clus1   up/up      169.254.3.8/23     node2
e0d     true
          node2_clus2   up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

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

**Show example**

```
cluster1::*> *cluster show*
Node            Health  Eligibility    Epsilon
--------------  -------  -------------  -------
node1           true     true          false
node2           true     true          false
```

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

**Show example**

```
cluster1::*> *cluster ping-cluster -node local*
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 e0b
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)
```

**For ONTAP 9.8 and later**

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

Enter: `system switch ethernet log setup-password`

```
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>
```

Followed by: `system switch ethernet log enable-collection`

```
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::*>
```

**For ONTAP 9.4 and later**

For ONTAP 9.4 and later, enable the cluster switch health monitor log collection feature for collecting switch-related log files using the commands:

`system cluster-switch log setup-password` and `system cluster-switch log enable-collection`

Enter: `system cluster-switch log setup-password`

```
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>
```

Followed by: `system cluster-switch log enable-collection`

```
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. |
|---|---|

# Ethernet Switch Health Monitoring log collection

The Ethernet switch health monitor (CSHM) is responsible for ensuring the operational health of Cluster and Storage network switches and collecting switch logs for debugging purposes. This procedure guides you through the process of setting up and starting the collection of detailed **Support** logs from the switch and starts an hourly collection of **Periodic** data that is collected by AutoSupport.

**Steps**

1. To set up log collection, run the following command for each switch. You are prompted to enter the switch name, username, and password for log collection.

   ```
   system switch ethernet log setup-password
   ```

   **Show example**

   ```
   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
   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   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
   Would you like to specify a user other than admin for log
   collection? {y|n}: n

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

2. To start log collection, run the following command, replacing DEVICE with the switch used in the previous command. This starts both types of log collection: the detailed **Support** logs and an hourly collection of

**Periodic** data.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

**Show example**

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*> system switch ethernet log modify -device cs2 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.
```

Wait for 10 minutes and then check that the log collection completes:

```
system switch ethernet log show
```

> ⚠️ If any of these commands return an error or if the log collection does not complete, contact NetApp support.

**Troubleshoot**

If you encounter any of the following error statuses reported by the log collection feature (visible in the output of `system switch ethernet log show`), try the corresponding debug steps:

| Log collection error status | Resolution |
|---|---|
| **RSA keys not present** | Regenerate ONTAP SSH keys. Contact NetApp support. |
| **switch password error** | Verify credentials, test SSH connectivity, and regenerate ONTAP SSH keys. Review switch documentation or contact NetApp support for instructions. |
| **ECDSA keys not present for FIPS** | If FIPS mode is enabled, ECDSA keys need to be generated on the switch before retrying. |

| pre-existing log found | Remove the previous log collection file on the switch. |
|---|---|
| switch dump log error | Ensure the switch user has log collection permissions. Refer to the prerequisites above. |

# Configure SNMPv3

Follow this procedure to configure SNMPv3, which supports Ethernet switch health monitoring (CSHM).

**About this task**

The following commands configure an SNMPv3 username on Cisco 92300YC switches:

- For **no authentication**: `snmp-server user SNMPv3_USER NoAuth`

- For **MD5/SHA authentication**: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`

- For **MD5/SHA authentication with AES/DES encryption**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

The following command configures an SNMPv3 username on the ONTAP side: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication -method usm -remote-switch-ipaddress ADDRESS`

The following command establishes the SNMPv3 username with CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

**Steps**

1. Set up the SNMPv3 user on the switch to use authentication and encryption:

   ```
   show snmp user
   ```

**Show example**

```
(sw1)(Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1)(Config)# show snmp user

----------------------------------------------------------------------
---------
                              SNMP USERS
----------------------------------------------------------------------
---------

User             Auth           Priv(enforce)   Groups
acl_filter
---------------- -------------- -------------- ---------------
-----------
admin            md5            des(no)         network-admin
SNMPv3User       md5            aes-128(no)     network-operator


----------------------------------------------------------------------
---------
    NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
----------------------------------------------------------------------
---------

User             Auth             Priv
---------------- ----------------- ------------

(sw1)(Config)#
```

2. Set up the SNMPv3 user on the ONTAP side:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

**Show example**

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212


Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configure CSHM to monitor with the new SNMPv3 user:

```
system switch ethernet show-all -device "sw1" -instance
```

**Show example**

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                Device Name: sw1
                                  IP Address: 10.231.80.212
                               SNMP Version: SNMPv2c
                              Is Discovered: true
    SNMPv2c Community String or SNMPv3 Username: cshm1!
                               Model Number: N9K-C92300YC
                              Switch Network: cluster-network
                            Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                   Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                      Source Of Switch Version: CDP/ISDP
                               Is Monitored ?: true
                  Serial Number of the Device: QTFCU3826001C
                                  RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Verify that the serial number to be queried with the newly created SNMPv3 user is the same as detailed in the previous step after the CSHM polling period has completed.

```
system switch ethernet polling-interval show
```

**Show example**

```
cluster1::*> system switch ethernet polling-interval show
          Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                    Device Name: sw1
                                     IP Address: 10.231.80.212
                                   SNMP Version: SNMPv3
                                  Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: SNMPv3User
                                   Model Number: N9K-C92300YC
                                 Switch Network: cluster-network
                               Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                        Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                         Source Of Switch Version: CDP/ISDP
                                 Is Monitored ?: true
                    Serial Number of the Device: QTFCU3826001C
                                    RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
```