NetApp

Configure software

Cluster and storage switches

NetApp
May 08, 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.

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 command outputs might vary depending on different releases of ONTAP.

Switch and node nomenclature

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=x h`

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

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

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

   ```
   set -privilege advanced
   ```

   The advanced prompt (`*>`) appears.

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

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

Show example

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

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

4 entries were displayed.
```

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

   a. Display the network port attributes:

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

Show example

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

Node: cluster1-02
                                                        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: cluster1-01
                                                        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
          cluster1-01_clus1  up/up        169.254.209.69/16
cluster1-01    e0a      true
          cluster1-01_clus2  up/up        169.254.49.125/16
cluster1-01    e0b      true
          cluster1-02_clus1  up/up        169.254.47.194/16
cluster1-02    e0a      true
          cluster1-02_clus2  up/up        169.254.19.183/16
cluster1-02    e0b      true

4 entries were displayed.
```

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

Show example

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

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

Show example

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


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

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

   `system switch ethernet log enable-collection`

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```

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

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

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

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::*>
```

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

Install the NX-OS software

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

Review requirements

What you'll need

- A current backup of the switch configuration.
- 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.
- Cisco Nexus 3000 Series Switches. Refer to 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

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 and RCF, 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

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

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

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

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

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:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


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

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

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

```
show version
```

Show example

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

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


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

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

Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
```

```
  Reason: Reset Requested by CLI command reload
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

5. Install the NX-OS image.

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

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         v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(01/28/2020)   no


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

```
Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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


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

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

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


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

  Device name: rtpnpi-mcc01-8200-ms-A1
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)

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

```
    Reason: Reset due to upgrade
    System version: 9.3(3)
    Service:

plugin
    Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

7. Upgrade the EPLD image and reboot the switch.

```
cs2# show version module 1 epld

EPLD Device                        Version
-----------------------------------------
MI   FPGA                          0x12
IO   FPGA                          0x11

cs2# install epld bootflash:n9000-epld.9.3.4.img module 1
Compatibility check:
Module         Type         Upgradable    Impact       Reason
------  -----------------  ----------   ----------   ------
    1        SUP           Yes          disruptive   Module
Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------  ----  ------------      ---------------   -----------
------------
    1   SUP   MI FPGA                    0x12          0x12
No
    1   SUP   IO FPGA                    0x11          0x12
Yes
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.
cs2#
```

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

Show example

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

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

Proceeding to upgrade Modules.

 Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
cs2#
```

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

Show example

```
cs2# show version module 1 epld

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

Install the Reference Configuration File (RCF)

Follow this procedure to install the RCF after setting up the Nexus 3232C switch for the first time.

You can also use this procedure to upgrade your RCF version. See the Knowledge Base article How to clear configuration on a Cisco interconnect switch while retaining remote connectivity for further information when upgrading your RCF.

Review requirements

What you'll need

- A current backup of the switch configuration.

- A fully functioning cluster (no errors in the logs or similar issues).

- The current Reference Configuration File (RCF).

- A console connection to the switch, required when installing the RCF.

- Cisco Ethernet switch page Consult the switch compatibility table for the supported ONTAP and RCF versions. Note that there can be command dependencies between the command syntax in the RCF and that found in versions of NX-OS.

- Cisco Nexus 3000 Series Switches. Refer to 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 file

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.

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 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.

Be sure to complete the procedure in Prepare to install NX-OS and RCF, and then follow the steps below.

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
----------- ------ ------------------------- ----------------
--------
cluster1-01/cdp
            e0a    cs1                        Ethernet1/7      N3K-
C3232C
            e0d    cs2                        Ethernet1/7      N3K-
C3232C
cluster1-02/cdp
            e0a    cs1                        Ethernet1/8      N3K-
C3232C
            e0d    cs2                        Ethernet1/8      N3K-
C3232C
cluster1-03/cdp
            e0a    cs1                        Ethernet1/1/1    N3K-
C3232C
            e0b    cs2                        Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
            e0a    cs1                        Ethernet1/1/2    N3K-
C3232C
            e0b    cs2                        Ethernet1/1/2    N3K-
C3232C
cluster1::*>
```

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

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

    `network port show -role cluster`

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/100000
healthy false
e0d      Cluster      Cluster          up   9000  auto/100000
healthy false


Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

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

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

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

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  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
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    10.233.205.92
NX3232C
        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
NX3232C
        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.

Show example

```
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.

Show example

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

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

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

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   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
8 entries were displayed.
cluster1::*>
```

6. 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::*>
```

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 reboot the switch.

> ⚠️ 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. Reboot the switch:

Show example

```
(cs2)# reload

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

9. Perform a basic setup of the switch. See Configure the 3232C cluster switch for details.

10. 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

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

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

11. 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

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

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

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

Show example

```
cs2# show banner motd

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

```
*
*     (4) Save running-configuration again
*********************************************************************
**********
```

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

13. 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.

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

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

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

15. 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
```

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

Show example

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

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

    a. Verify that e0d ports are up and healthy across all nodes in the cluster:

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

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

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

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-C3232C
             e0d    cs2                       Ethernet1/7
N3K-C3232C
cluster01-2/cdp
             e0a    cs1                       Ethernet1/8
N3K-C3232C
             e0d    cs2                       Ethernet1/8
N3K-C3232C
cluster01-3/cdp
             e0a    cs1                       Ethernet1/1/1
N3K-C3232C
             e0b    cs2                       Ethernet1/1/1
N3K-C3232C
cluster1-04/cdp
             e0a    cs1                       Ethernet1/1/2
N3K-C3232C
             e0b    cs2                       Ethernet1/1/2
N3K-C3232C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                         Type              Address
Model
-------------------------- ----------------- -----------------
-----
cs1                            cluster-network   10.233.205.90
N3K-C3232C
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                  9.3(4)
    Version Source: CDP

cs2                            cluster-network   10.233.205.91
```

```
N3K-C3232C
      Serial Number: FOXXXXXXXGS
        Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
     Version Source: CDP

2 entries were displayed.
```

(i) 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.
```

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

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

Show example

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

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

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

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

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     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
8 entries were displayed.
cluster1::*>
```

20. Verify that the cluster is healthy:

```
cluster show
```

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

21. Repeat Steps 7 to 15 on switch cs1.

22. Enable auto-revert on the cluster LIFs.

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

23. 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
```

24. Verify that the switch ports connected to the cluster ports are 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)  --
.
.
```

25. 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#
```

26. 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: `network interface revert -vserver` *vserver_name* `-lif` *lif_name*

27. 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::*>
```

28. Ping the remote cluster interfaces to verify connectivity:

```
cluster ping-cluster -node local
```

Show example

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

Ethernet Switch Health Monitoring log collection

You can use the log collection feature to collect switch-related log files in ONTAP. 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.

Before you begin

- Verify that you have set up your environment using the Cisco 3232C cluster switch **CLI**.

- Switch health monitoring must be enabled for the switch. Verify this by ensuring the `Is Monitored:` field is set to **true** in the output of the `system switch ethernet show` command.

Steps

1. Create a password for the Ethernet switch health monitor log collection feature:

   `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.

Troubleshooting

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 the 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 3232C 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: N3K-C3232C
                                 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: N3K-C3232C
                             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::*>
```