Software konfigurieren

Cluster and storage switches

NetApp
April 25, 2024

Inhalt

Software konfigurieren

Vorbereiten der Installation der NX-OS-Software und der Referenzkonfigurationsdatei (RCF)

Bevor Sie die NX-OS-Software und die RCF-Datei (Reference Configuration File) installieren, gehen Sie wie folgt vor:

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster-Interconnect-Ports `e0a` Und `e0b`.

Siehe "Hardware Universe" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.

> Die Ausgaben für die Befehle können je nach verschiedenen Versionen von ONTAP variieren.

Switch- und Node-Terminologie

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches lauten `cs1` Und `cs2`.
- Die Node-Namen sind `cluster1-01` Und `cluster1-02`.
- Die LIF-Namen des Clusters sind `cluster1-01_clus1` Und `cluster1-01_clus2` Für Clustered 1-01 und `cluster1-02_clus1` Und `cluster1-02_clus2` Für Clustered 1-02.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=x h`

   Wobei *x* die Dauer des Wartungsfensters in Stunden ist.

   > Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

   ```
   set -privilege advanced
   ```

   Die erweiterte Eingabeaufforderung (`*>`Erscheint.

3. Zeigen Sie an, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster Interconnect-Switch konfiguriert sind:

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

   Beispiel anzeigen

   ```
   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. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.

   a. Zeigen Sie die Attribute des Netzwerkports an:

      ```
      network port show –ipspace Cluster
      ```

Beispiel anzeigen

```
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.
```

a. Zeigt Informationen zu den LIFs an: `network interface show -vserver Cluster`

Beispiel anzeigen

```
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 für die Remote-Cluster-LIFs: `cluster ping-cluster -node node-name`

Beispiel anzeigen

```
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. Überprüfen Sie das `auto-revert` Befehl ist für alle Cluster-LIFs aktiviert: `network interface show -vserver Cluster -fields auto-revert`

Beispiel anzeigen

```
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. Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle: `system switch ethernet log setup-password`

   `system switch ethernet log enable-collection`

Beispiel anzeigen

```
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::*>
```

Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

8. Aktivieren Sie bei Patch-Releases von ONTAP Releases 9.5P16, 9.6P12 und 9.7P10 sowie höher die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien: `system cluster-switch log setup-password`

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

Beispiel anzeigen

```
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::*>
```

Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Installieren Sie die NX-OS-Software

Mithilfe dieser Vorgehensweise können Sie die NX-OS-Software auf dem Nexus 3232C-Cluster-Switch installieren.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- "Cisco Ethernet Switch Seite". In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.
- "Switches Der Cisco Nexus 3000-Serie". Ausführliche Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website.

Installieren Sie die Software

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Führen Sie den Vorgang in durch "Bereiten Sie sich auf die Installation von NX-OS und RCF vor", Und dann folgen Sie den Schritten unten.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung mit dem Server, der die NX-OS-Software und die RCF hostet.

   Beispiel anzeigen

   In diesem Beispiel wird überprüft, ob der Switch den Server unter der IP-Adresse 172.19.2 erreichen kann:

   ```
   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. Kopieren Sie die NX-OS-Software und EPLD-Bilder auf den Nexus 3232C-Switch.

Beispiel anzeigen

```
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. Überprüfen Sie die laufende Version der NX-OS-Software:

   ```
   show version
   ```

Beispiel anzeigen

```
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. Installieren Sie das NX-OS Image.

   Durch die Installation der Image-Datei wird sie bei jedem Neustart des Switches geladen.

Beispiel anzeigen

```
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. Überprüfen Sie nach dem Neustart des Switches die neue Version der NX-OS-Software: `show version`

Beispiel anzeigen

```
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. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

Beispiel anzeigen

```
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. Melden Sie sich nach dem Neustart des Switches erneut an, aktualisieren Sie das goldene EPLD-Bild und starten Sie den Switch erneut.

Beispiel anzeigen

```
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. Melden Sie sich nach dem Neustart des Switches an, um zu überprüfen, ob die neue EPLD-Version erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld

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

Was kommt als Nächstes?

"Installieren Sie die RCF-Konfigurationsdatei"

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Gehen Sie folgendermaßen vor, um den RCF nach dem ersten Einrichten des Nexus 3232C-Switch zu installieren.

Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren. Weitere Informationen finden Sie im Knowledge Base-Artikel "Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung" Weitere Informationen zum Upgrade Ihres RCF.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Die aktuelle Referenzkonfigurationsdatei (RCF).
- Eine Konsolenverbindung mit dem Switch, die bei der Installation des RCF erforderlich ist.
- "Cisco Ethernet Switch Seite" In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen. Beachten Sie, dass es Abhängigkeiten zwischen der Befehlssyntax im RCF und der in Versionen von NX-OS gibt.
- "Switches Der Cisco Nexus 3000-Serie". Ausführliche Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website.

Installieren Sie die Datei

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches lauten `cs1` Und `cs2`.
- Die Node-Namen sind `cluster1-01`, `cluster1-02`, `cluster1-03`, und `cluster1-04`.
- Die LIF-Namen des Clusters sind `cluster1-01_clus1`, `cluster1-01_clus2`, `cluster1-02_clus1`, `cluster1-02_clus2` , `cluster1-03_clus1`, `cluster1-03_clus2`, `cluster1-04_clus1`, und

`cluster1-04_clus2`.

- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Führen Sie den Vorgang in durch "Bereiten Sie sich auf die Installation von NX-OS und RCF vor", Und dann folgen Sie den Schritten unten.

Schritte

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

   ```
   network device-discovery show
   ```

Beispiel anzeigen

```
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. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

   a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

Beispiel anzeigen

```
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. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

Beispiel anzeigen

```
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. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

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

Beispiel anzeigen

```
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. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

4. Fahren Sie beim Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

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

5. Überprüfen Sie, ob die Cluster-Ports zu den Ports migriert wurden, die auf Cluster-Switch cs1 gehostet werden. Dies kann einige Sekunden dauern.

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

   Beispiel anzeigen

   ```
   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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

   ```
   cluster show
   ```

Beispiel anzeigen

```
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. Wenn Sie dies noch nicht getan haben, speichern Sie eine Kopie der aktuellen Switch-Konfiguration, indem Sie die Ausgabe des folgenden Befehls in eine Textdatei kopieren:

   ```
   show running-config
   ```

8. Reinigen Sie die Konfiguration auf Switch cs2, und starten Sie den Switch neu.

   > Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

   a. Konfiguration bereinigen:

      Beispiel anzeigen

      ```
      (cs2)# write erase

      Warning: This command will erase the startup-configuration.

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

   b. Starten Sie den Switch neu:

      Beispiel anzeigen

      ```
      (cs2)# reload

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

9. Führen Sie eine grundlegende Einrichtung des Switches durch. Siehe "Konfigurieren Sie den 3232C-Cluster-Switch" Entsprechende Details.

10. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 3000-Serie NX-OS Command Reference" Leitfäden.

    Beispiel anzeigen

    Dieses Beispiel zeigt, dass TFTP zum Kopieren eines RCF auf den Bootflash auf Switch cs2 verwendet wird:

    ```
    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. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

    Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 3000-Serie NX-OS Command Reference" Leitfäden.

    Beispiel anzeigen

    Dieses Beispiel zeigt die RCF-Datei `Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt` Installation auf Schalter cs2:

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

12. Untersuchen Sie die Bannerausgabe aus dem `show banner motd` Befehl. Sie müssen die Anweisungen unter **wichtige Hinweise** lesen und befolgen, um sicherzustellen, dass der Schalter ordnungsgemäß konfiguriert und betrieben wird.

Beispiel anzeigen

```
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
**********************************************************************
**********
```

Beim ersten Anwenden des RCF wird die Meldung **ERROR: Failed to write VSH befiehlt** erwartet und kann ignoriert werden.

13. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

    ```
    show running-config
    ```

    Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

    - Das RCF-Banner
    - Die Node- und Port-Einstellungen
    - Anpassungen

      Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

14. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Start-config-Datei.

    Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 3000-Serie NX-OS Command Reference" Leitfäden.

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

15. Schalter cs2 neu starten. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

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

16. Wenden Sie dieselbe RCF an, und speichern Sie die ausgeführte Konfiguration ein zweites Mal.

Beispiel anzeigen

```
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. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

    a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß sind:

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

Beispiel anzeigen

```
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. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch cs2 an, da LIFs nicht auf e0d homed sind).

Beispiel anzeigen

```
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.
```

Je nach der zuvor auf dem Switch geladenen RCF-Version können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten

```
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.
```

Es kann bis zu 5 Minuten dauern, bis die Cluster-Nodes einen ordnungsgemäßen Zustand melden.

18. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

Im folgenden Beispiel wird die Ausgabe des Schnittstellenbeispiels aus Schritt 1 verwendet:

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

19. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf dem Switch cs2 gehostet werden. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

```
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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

    `cluster show`

Beispiel anzeigen

```
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. Wiederholen Sie die Schritte 7 bis 15 am Schalter cs1.
22. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

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

23. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

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

24. Vergewissern Sie sich, dass die mit den Cluster-Ports verbundenen Switch-Ports aktiv sind.

Beispiel anzeigen

```
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. Stellen Sie sicher, dass die ISL zwischen cs1 und cs2 funktionsfähig ist:

```
show port-channel summary
```

Beispiel anzeigen

```
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. Vergewissern Sie sich, dass die Cluster-LIFs auf ihren Home-Port zurückgesetzt wurden:

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

Beispiel anzeigen

```
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::*>
```

Wenn keine Cluster-LIFS an die Home-Ports zurückgegeben wurden, setzen Sie sie manuell zurück: `network interface revert -vserver vserver_name -lif lif_name`

27. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

    `cluster show`

Beispiel anzeigen

```
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 für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität:

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

Beispiel anzeigen

```
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)
```

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Sie können die Protokollerfassungsfunktion verwenden, um Switch-bezogene Protokolldateien in ONTAP zu sammeln. Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Ihre Umgebung über den Cisco 3232C Cluster Switch * CLI * eingerichtet haben.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

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

Beispiel anzeigen

```
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. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

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

Beispiel anzeigen

```
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.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```

Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um weitere Informationen zu erhalten.
ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.

Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Cisco 3232C-Switches konfiguriert:

- Für **keine Authentifizierung**: `snmp-server user SNMPv3_USER NoAuth`
- Für * MD5/SHA-Authentifizierung*: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication-method usm -remote-switch-ipaddress ADDRESS`

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

   ```
   show snmp user
   ```

Beispiel anzeigen

```
(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. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

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

Beispiel anzeigen

```
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. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

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

Beispiel anzeigen

```
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. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

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

Beispiel anzeigen

```
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::*>
```