配置软件

Cluster and storage switches

NetApp
April 25, 2024

目录

配置软件

准备安装NX-OS软件和参考配置文件(Reference Configuration File、RCF)

在安装NX-OS软件和参考配置文件(Reference Configuration File、RCF)之前、请遵循此操作步骤。

您需要的内容

- 一个完全正常运行的集群(日志中没有错误或类似问题)。
- 可从获取相应的软件和升级指南 "Cisco Nexus 9000 系列交换机"。

关于示例

此操作步骤中的示例使用两个节点。这些节点使用两个10GbE集群互连端口 `e0a` 和 `e0b`。请参见 "Hardware Universe" 验证平台上的集群端口是否正确。

此操作步骤中的示例使用以下交换机和节点命名：

- 这两台 Cisco 交换机的名称分别为 `CS1` 和 `CS2` 。
- 节点名称为 `node1` 和 `node2` 。
- 集群 LIF 名称是 node1 的 `node1_clus1` 和 `node1_clus2` ， node2 的 `node2_clus1` 和 `node2_clus2` 。
- `cluster1 ：：： * >` 提示符指示集群的名称。

关于此任务

操作步骤要求同时使用 ONTAP 命令和 Cisco Nexus 9000 系列交换机命令；除非另有说明，否则使用 ONTAP 命令。根据不同版本的 ONTAP ，命令输出可能会有所不同。

步骤

1. 将权限级别更改为高级，在系统提示您继续时输入 * y * ：

   ```
   set -privilege advanced
   ```

   此时将显示高级提示符（`*>`）。

2. 如果在此集群上启用了 AutoSupport ，则通过调用 AutoSupport 消息禁止自动创建案例：

   ```
   ssystem node AutoSupport invoke -node * -type all -message MAINT=xh
   ```

   其中 *x* 是维护时段的持续时间，以小时为单位。

   > AutoSupport 消息会通知技术支持此维护任务，以便在维护窗口期间禁止自动创建案例。

   以下命令将禁止自动创建案例 2 小时：

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

3. 显示在每个集群互连交换机的每个节点上配置了多少个集群互连接口： `network device-discovery show -protocol cdp`

   显示示例

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

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

4 entries were displayed.
```

4. 检查每个集群接口的管理或运行状态。

   a. 显示网络端口属性： `network port show -ipspace Cluster`

显示示例

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

Node: node2
                                                        Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: node1
                                                        Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. 显示有关 LIF 的信息： `network interface show - Vserver Cluster`

显示示例

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

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

4 entries were displayed.
```

5. 对远程集群 LIF 执行 Ping 操作：

   `cluster ping-cluster -node node-name`

显示示例

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

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

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

6. 验证是否已在所有集群 LIF 上启用 auto-revert 命令：

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

显示示例

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

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

4 entries were displayed.
```

7. 对于 ONTAP 9.4 及更高版本，请使用以下命令启用集群交换机运行状况监控器日志收集功能以收集交换机相关的日志文件：

   `ssystem cluster-switch log setup-password` 和 `ssystem cluster-switch log enable-Collection`

显示示例

```
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::*>
```

如果其中任何一个命令返回错误，请联系 NetApp 支持部门。

下一步是什么？

"安装 NX-OS 软件"。

安装 NX-OS 软件

按照此操作步骤 在Nexus 92300YC交换机上安装NX-OS软件。

NX-OS 是 Cisco Systems 提供的 Nexus 系列以太网交换机和 MDS 系列光纤通道（ FC ）存储区域网络交换机的网络操作系统。

查看要求

支持的端口和节点连接

- Nexus 92300YC 交换机支持的交换机间链路（ ISL ）为端口 1/65 和 1/66 。
- Nexus 92300YC 交换机支持的节点连接为端口 1/1 到 1/66 。

您需要的内容

- 适用于NetApp 支持站点 中交换机的NetApp Cisco NX-OS软件、可从获取 "mysupport.netapp.com"
- 一个完全正常运行的集群(日志中没有错误或类似问题)。
- "Cisco 以太网交换机页面"。有关支持的ONTAP 和NX-OS版本、请参见交换机兼容性表。

安装软件

此操作步骤中的示例使用两个节点，但一个集群中最多可以有 24 个节点。

关于示例

此操作步骤中的示例使用以下交换机和节点命名：

- Nexus 92300YC 交换机名称为 `CS1` 和 `CS2` 。
- 此操作步骤中使用的示例将在第二个交换机 _* CS2* 上启动升级。 _
- 集群 LIF 名称是 node1 的 `node1_clus1` 和 `node1_clus2` ， node2 的 `node2_clus1` 和 `node2_clus2` 。
- IP 空间名称是 `Cluster` 。
- `cluster1 ：：： * >` 提示符指示集群的名称。
- 每个节点上的集群端口分别命名为 `e0a` 和 `e0b` 。

  请参见 "Hardware Universe^ _" 您的平台支持的实际集群端口。

步骤

1. 将集群交换机连接到管理网络。
2. 使用 `ping` 命令验证与托管 NX-OS 软件和 RCF 的服务器的连接。

显示示例

此示例验证交换机是否可以通过 IP 地址 172.19.2.1 访问服务器：

```
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. 将 NX-OS 软件和 EPLD 映像复制到 Nexus 92300YC 交换机。

显示示例

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.2.2.bin  /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.2.2.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.2.2.img  /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. 验证正在运行的 NX-OS 软件版本：

   s如何使用版本

显示示例

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

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


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

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

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

```
  System version: 9.2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

5. 安装 NX-OS 映像。

   安装映像文件会导致每次重新启动交换机时加载该映像文件。

显示示例

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

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

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

Verifying image type.
[] 100% -- SUCCESS

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

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

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

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



Compatibility check is done:
Module  bootable       Impact     Install-type  Reason
------  --------  --------------- ------------  ------
  1       yes      disruptive         reset     default upgrade is
not hitless



Images will be upgraded according to following table:

Module   Image         Running-Version(pri:alt            New-
Version         Upg-Required
------  --------  ---------------------------------------
------------------  ------------
  1       nxos                                  9.2(1)
9.2(2)         yes
  1       bios    v05.31(05/17/2018):v05.28(01/18/2018)
v05.33(09/08/2018)       yes
```

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


Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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

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

6. 在交换机重新启动后验证 NX-OS 软件的新版本：

   s如何使用版本

显示示例

```
cs2# show version

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

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


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

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

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

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

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

7. 升级 EPLD 映像并重新启动交换机。

显示示例

```
cs2# show version module 1 epld

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

cs2# install epld bootflash:n9000-epld.9.2.2.img module 1
Compatibility check:
Module        Type         Upgradable        Impact   Reason
------  -----------------  ----------    ----------   ------
     1            SUP           Yes       disruptive  Module
Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------  ----  -------------      ---------------   -----------
------------
     1   SUP  MI FPGA                   0x07        0x07
No
     1   SUP  IO FPGA                   0x17        0x19
Yes
     1   SUP  MI FPGA2                  0x02        0x02
No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

```
      1          SUP          Success


EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

8. 交换机重新启动后，重新登录并验证是否已成功加载新版本的 EPLD 。

显示示例

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

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

下一步是什么？

"安装参考配置文件"

安装参考配置文件（RCF）

首次设置 Nexus 92300YC 交换机后，您可以安装 RCF 。您也可以使用此操作步骤升级 RCF 版本。

关于此任务

此操作步骤中的示例使用以下交换机和节点命名：

- 这两台 Cisco 交换机的名称分别为 `CS1` 和 `CS2` 。
- 节点名称为 `node1` 和 `node2` 。
- 集群LIF名称是 `node1_clus1`， `node1_clus2`， `node2_clus1`，和 `node2_clus2`。
- `cluster1 ::: * >` 提示符指示集群的名称。

- 操作步骤 需要同时使用ONTAP 命令和 "Cisco Nexus 9000 系列交换机"；除非另有说明、否则使用ONTAP 命令。
- 在执行此操作步骤 之前、请确保已为交换机配置创建备份。
- 在此操作步骤 期间、不需要可操作的交换机间链路(ISL)。这是设计上的原因、因为RCF版本更改可能会暂时影响ISL连接。为了确保集群无中断运行、以下操作步骤 会在对目标交换机执行步骤时将所有集群LIF迁移到运行中的配对交换机。

步骤

1. 显示连接到集群交换机的每个节点上的集群端口： `network device-discovery show`

   显示示例

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

2. 检查每个集群端口的管理和运行状态。

   a. 验证所有集群端口是否均已启动且状态正常： `network port show -ipspace Cluster`

显示示例

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

Node: node1

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

Node: node2

Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
cluster1::*>
```

b. 验证所有集群接口（LIF）是否均位于主端口上：`network interface show -vserver Cluster`

显示示例

```
cluster1::*> *network interface show -vserver Cluster*
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            node1_clus1        up/up      169.254.3.4/23    node1
e0c     true
            node1_clus2        up/up      169.254.3.5/23    node1
e0d     true
            node2_clus1        up/up      169.254.3.8/23    node2
e0c     true
            node2_clus2        up/up      169.254.3.9/23    node2
e0d     true
cluster1::*>
```

c. 验证集群是否同时显示两个集群交换机的信息： `ssystem cluster-switch show -is -monitoring-enableed-Operational true`

显示示例

```
cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.233.205.92
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.93
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

3. 在集群 LIF 上禁用自动还原。

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

4. 在集群交换机 CS2 上，关闭连接到节点集群端口的端口。

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. 验证集群端口是否已迁移到集群交换机 CS1 上托管的端口。这可能需要几秒钟的时间。 `network interface show -vserver Cluster`

显示示例

```
cluster1::*> *network interface show -vserver Cluster*
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1       up/up      169.254.3.4/23     node1
e0c     true
            node1_clus2       up/up      169.254.3.5/23     node1
e0c     false
            node2_clus1       up/up      169.254.3.8/23     node2
e0c     true
            node2_clus2       up/up      169.254.3.9/23     node2
e0c     false
cluster1::*>
```

6. 验证集群是否运行正常： `cluster show`

显示示例

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

7. 如果尚未保存当前交换机配置的副本、请将以下命令的输出复制到文本文件中：

   s如何运行配置

8. 清理交换机 CS2 上的配置并执行基本设置。

   更新或应用新 RCF 时，必须擦除交换机设置并执行基本配置。您必须连接到交换机串行控制台端口才能重新设置交换机。

   a. 清理配置：

显示示例

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

b. 重新启动交换机：

显示示例

```
(cs2)# reload

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

9. 使用以下传输协议之一将 RCF 复制到交换机 CS2 的启动闪存： FTP ， TFTP ， SFTP 或 SCP 。有关 Cisco 命令的详细信息，请参见中的相应指南 "Cisco Nexus 9000 系列交换机" 指南。

   此示例显示了使用 TFTP 将 RCF 复制到交换机 CS2 上的 bootflash 。

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: /code/Nexus_92300YC_RCF_v1.0.2.txt
Enter hostname for the tftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
tftp> progress
Progress meter enabled
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin
/code/Nexus_92300YC_R  100% 9687   530.2KB/s   00:00
tftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

10. 将先前下载的 RCF 应用于 bootflash 。

    有关 Cisco 命令的详细信息，请参见中的相应指南 "Cisco Nexus 9000 系列交换机" 指南。

    此示例显示了RCF文件 `Nexus_92300YC_RCF_v1.0.2.txt` 安装在交换机CS2上：

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

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

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

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

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

...

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

11. 在交换机上验证 RCF 是否已成功合并：

    s如何运行配置

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

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

feature lacp

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

banner motd #

*
*
*  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
*
*
*
*  Ports 1/1  - 1/48: 10GbE Intra-Cluster Node Ports
*
*  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
*
*  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
*
*
*
```

首次应用 RCF 时，系统会显示 * 错误：无法写入 VSH 命令 * 消息，可以忽略该消息。

1. 【第12步】验证RCF文件是否为正确的较新版本： `show running-config`

在检查输出以确认您的 RCF 正确无误时，请确保以下信息正确无误：

- RCF 横幅
- 节点和端口设置
- 自定义

  输出因站点配置而异。检查端口设置，并参阅发行说明，了解您安装的 RCF 的任何特定更改。

2. 验证 RCF 版本和交换机设置是否正确后，将 running-config 文件复制到 startup-config 文件。

   有关 Cisco 命令的详细信息，请参见中的相应指南 "Cisco Nexus 9000 系列交换机" 指南。

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

3. 重新启动交换机 CS2 。您可以忽略交换机重新启动时在节点上报告的 " 集群端口关闭 " 事件。

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

4. 验证集群上集群端口的运行状况。

   a. 验证集群中所有节点上的 e0d 端口是否均已启动且运行正常： `network port show -ipspace Cluster`

显示示例

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

Node: node1

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

Node: node2

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

b. 从集群验证交换机运行状况（此操作可能不会显示交换机 CS2 ，因为 LIF 不驻留在 e0d 上）。

显示示例

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

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
------------
cs1                         cluster-network    10.233.205.90
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

根据先前加载在 CS1 交换机控制台上的 RCF 版本，您可能会在该交换机控制台上看到以下输出

```
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.
```

5. 在集群交换机 CS1 上，关闭连接到节点集群端口的端口。

   以下示例使用步骤 1 中的接口示例输出：

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

6. 验证集群 LIF 是否已迁移到交换机 CS2 上托管的端口。这可能需要几秒钟的时间。 `network interface show -vserver Cluster`

   显示示例

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

7. 验证集群是否运行正常： `cluster show`

显示示例

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

8. 对交换机 CS1 重复步骤 7 至 14 。
9. 在集群 LIF 上启用自动还原。

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

10. 重新启动交换机 CS1 。执行此操作可触发集群 LIF 还原到其主端口。您可以忽略交换机重新启动时在节点上报告的 " 集群端口关闭 " 事件。

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

11. 验证连接到集群端口的交换机端口是否已启动。

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

12. 验证 CS1 和 CS2 之间的 ISL 是否正常运行： s如何执行端口通道摘要

显示示例

```
cs1# *show port-channel summary*
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
----------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
----------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
cs1#
```

13. 验证集群 LIF 是否已还原到其主端口： `network interface show -vserver Cluster`

显示示例

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

14. 验证集群是否运行正常： `cluster show`

显示示例

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

15. 对远程集群接口执行 Ping 操作以验证连接： `cluster ping-cluster -node local`

显示示例

```
cluster1::*> *cluster ping-cluster -node local*
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

适用于**ONTAP 9.8**及更高版本

对于 ONTAP 9.8 及更高版本，使用以下命令启用集群交换机运行状况监控器日志收集功能以收集交换机相关的日志文件： `system switch ethernet log setup-password` 和 `system switch ethernet log enable-collection`

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

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

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

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

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

cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

后跟： `system switch ethernet log enable-collection`

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

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

Enabling cluster switch log collection.

cluster1::*>
```

适用于**ONTAP 9.4**及更高版本

对于 ONTAP 9.4 及更高版本，请使用以下命令启用集群交换机运行状况监控器日志收集功能以收集交换机相关的日志文件：

`ssystem cluster-switch log setup-password` 和 `ssystem cluster-switch log enable-Collection`

输入： `ssystem cluster-switch log setup-password`

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

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```

如果其中任何一个命令返回错误，请联系 NetApp 支持部门。

以太网交换机运行状况监控日志收集

以太网交换机运行状况监控器(CSHM)负责确保集群和存储网络交换机的运行状况、并收集交换机日志以进行调试。此操作步骤将引导您完成设置和开始从交换机收集详细的*Support*日志的过程，并开始每小时收集由AutoSupport收集的*定期*数据。

步骤

1. 要设置日志收集、请对每个交换机运行以下命令。系统会提示您输入交换机名称、用户名和密码以收集日志。

   s系统交换机以太网日志设置密码

   显示示例

```
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. 要开始收集日志、请运行以下命令、将device替换为上一命令中使用的交换机。这将开始两种类型的日志收集：详细的*Support*日志和每小时收集*定期*数据。

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

显示示例

```
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.
```

等待10分钟、然后检查日志收集是否完成：

```
system switch ethernet log show
```

> 如果其中任一命令返回错误或日志收集未完成、请联系NetApp支持部门。

故障排除

如果遇到日志收集功能报告的以下任一错误状态(在的输出中可见) `system switch ethernet log show`)、请尝试相应的调试步骤：

日志收集错误状态	分辨率
RSA密钥不存在	重新生成ONTAP SSH密钥。请联系NetApp支持部门。
交换机密码错误	验证凭据、测试SSH连接并重新生成ONTAP SSH密钥。查看交换机文档或联系NetApp支持部门以获取相关说明。
对于**FIPS**，ECDSA密钥不存在	如果启用了FIPS模式、则需要在重试之前在交换机上生成ECDSA密钥。
已找到已有日志	删除交换机上先前的日志收集文件。

交换机转储日志错误	确保交换机用户具有日志收集权限。请参阅上述前提条件。

配置SNMPv3

按照此操作步骤配置SNMPv3、此SNMPv3支持以太网交换机运行状况监控(CSHM)。

关于此任务

以下命令可在Cisco 92300YC交换机上配置SNMPv3用户名：

- 对于*no authentication (无身份验证)*： `snmp-server user SNMPv3_USER NoAuth`
- 对于*MD5/SHA身份验证*： `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- 对于采用AES/DES加密的*MD5/SHA身份验证*： `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

以下命令会在ONTAP 端配置SNMPv3用户名：`cluster1：：：*> security login create -user-or -group-name SNMPv3用户-application snmp -authentication-method USM -remote-switch -ipaddress address`

以下命令将使用CSHM建立SNMPv3用户名： `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

步骤

1. 在交换机上设置SNMPv3用户以使用身份验证和加密：

   ```
   show snmp user
   ```

显示示例

```
(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. 在ONTAP 端设置SNMPv3用户：

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

显示示例

```
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. 将CSHM配置为使用新SNMPv3用户进行监控：

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

显示示例

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

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

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

4. 确认要使用新创建的SNMPv3用户查询的序列号与CSHM轮询周期完成后上一步中详述的序列号相同。

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

显示示例

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

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

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

cluster1::*>
```