Configurar el software

Install and maintain

NetApp
October 24, 2025

This PDF was generated from https://docs.netapp.com/es-es/ontap-systems-switches/switch-cisco-92300/configure-software-overview-92300-cluster.html on October 24, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configurar el software . . . 1
- Flujo de trabajo de instalación de software para conmutadores de clúster Cisco Nexus 92300YC . . . 1
- Configure el switch Cisco Nexus 92300YC . . . 1
- Preparar la instalación del software NX-OS y del archivo de configuración de referencia (RCF) . . . 5
- Instale el software NX-OS . . . 11
  - Revise los requisitos . . . 11
  - Instale el software . . . 11
- Instalación del archivo de configuración de referencia (RCF) . . . 21
- Compruebe su configuración SSH . . . 39

Configurar el software

Flujo de trabajo de instalación de software para conmutadores de clúster Cisco Nexus 92300YC

Para instalar y configurar el software de un conmutador Cisco Nexus 92300YC e instalar o actualizar el archivo de configuración de referencia (RCF), siga estos pasos:

1. **"Configure el switch"**

Configurar el conmutador de clúster 92300YC.

2. **"Prepárese para instalar el software NX-OS y RCF"**

El software Cisco NX-OS y los archivos de configuración de referencia (RCF) deben estar instalados en los conmutadores de clúster Cisco 92300YC.

3. **"Instale o actualice el software NX-OS"**

Descargue e instale o actualice el software NX-OS en el conmutador de clúster Cisco 392300YC.

4. **"Instale el RCF"**

Instale el RCF después de configurar el conmutador Cisco 92300YC por primera vez.

5. **"Compruebe la configuración de SSH"**

Verifique que SSH esté habilitado en los conmutadores para usar el Monitor de estado del conmutador Ethernet (CSHM) y las funciones de recopilación de registros.

Configure el switch Cisco Nexus 92300YC

Siga este procedimiento para configurar y configurar el switch Cisco Nexus 92300YC.

Pasos

1. Conecte el puerto serie a un host o puerto serie.
2. Conecte el puerto de gestión (en el lado que no sea un puerto del switch) a la misma red donde esté ubicado el servidor SFTP.
3. En la consola, configure los ajustes de serie del lado del host:
    - 9600 baudios
    - 8 bits de datos
    - 1 bit de parada
    - paridad: none

- control de flujo: ninguno

4. Cuando se arranca por primera vez o se reinicia después de borrar la configuración en ejecución, el switch Nexus 92300YC recorre un ciclo de arranque. Interrumpa este ciclo escribiendo **yes** para cancelar la alimentación en el aprovisionamiento automático.

   Aparecerá la configuración de la cuenta de administración del sistema.

   Muestra el ejemplo

   ```
   $ VDC-1 %$ %POAP-2-POAP_INFO:   - Abort Power On Auto Provisioning
   [yes - continue with normal setup, skip - bypass password and basic
   configuration, no - continue with Power On Auto Provisioning]
   (yes/skip/no)[no]: y
   Disabling POAP.......Disabling POAP
   2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please
   wait... (This may take 5-15 minutes)

             ---- System Admin Account Setup ----

   Do you want to enforce secure password standard (yes/no) [y]:
   ```

5. Escriba **y** para aplicar el estándar de contraseña segura:

   ```
   Do you want to enforce secure password standard (yes/no) [y]: y
   ```

6. Introduzca y confirme la contraseña para el administrador del usuario:

   ```
   Enter the password for "admin":
   Confirm the password for "admin":
   ```

7. Escriba **yes** para abrir el cuadro de diálogo Configuración básica del sistema.

Muestra el ejemplo

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):
```

8. Cree otra cuenta de inicio de sesión:

```
Create another login account (yes/no) [n]:
```

9. Configure las cadenas de comunidad SNMP de solo lectura y de lectura y escritura:

```
Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:
```

10. Configure el nombre del switch del clúster:

```
Enter the switch name : cs2
```

11. Configure la interfaz de gestión fuera de banda:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address : 172.22.133.216

Mgmt0 IPv4 netmask : 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : 172.22.128.1
```

12. Configure las opciones avanzadas de IP:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Configurar servicios Telnet:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Configure los servicios SSH y las claves SSH:

```
Enable the ssh service? (yes/no) [y]: y

       Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa

       Number of rsa key bits <1024-2048> [1024]: 2048
```

15. Configurar otras opciones:

```
Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L2]: L2

  Configure default switchport interface state (shut/noshut) [noshut]:
noshut

  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: strict
```

16. Confirme la información del switch y guarde la configuración:

```
Would you like to edit the configuration? (yes/no) [n]: n

Use this configuration and save it? (yes/no) [y]: y

[] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

El futuro

"Prepárese para instalar el software NX-OS y RCF".

Preparar la instalación del software NX-OS y del archivo de configuración de referencia (RCF)

Antes de instalar el software NX-OS y el archivo de configuración de referencia (RCF), siga este procedimiento.

Antes de empezar

Asegúrese de tener lo siguiente:

- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- Guías de software y actualización adecuadas, disponibles en "Switches Cisco Nexus serie 9000".

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan dos nodos. Estos nodos utilizan dos puertos de interconexión de clúster de 10 GbE `e0a` y.. `e0b`. Consulte "Hardware Universe" para verificar los puertos de clúster correctos en sus plataformas.

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches Cisco son `cs1` y.. `cs2`.
- Los nombres de nodo son `node1` y.. `node2`.
- Los nombres de LIF del clúster son `node1_clus1` y.. `node1_clus2` para los nodos 1 y `node2_clus1` y.. `node2_clus2` para el 2.
- La `cluster1::*>` prompt indica el nombre del clúster.

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 9000; los comandos de la ONTAP se usan a menos que se indique lo contrario. Los resultados del comando pueden variar en función de las diferentes versiones de ONTAP.

Pasos

1. Cambie el nivel de privilegio a avanzado, introduciendo **y** cuando se le solicite continuar:

   ```
   set -privilege advanced
   ```

El aviso avanzado (`*>`) aparece.

2. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport:

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

   donde *x* es la duración de la ventana de mantenimiento en horas.

   > El mensaje de AutoSupport notifica al soporte técnico de esta tarea de mantenimiento para que la creación automática de casos se suprima durante la ventana de mantenimiento.

   El siguiente comando suprime la creación automática de casos durante dos horas:

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

3. Muestre cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster: `network device-discovery show -protocol cdp`

   Muestra el ejemplo

   ```
   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. Compruebe el estado administrativo u operativo de cada interfaz de clúster.

   a. Mostrar los atributos del puerto de red: `network port show –ipspace Cluster`

Muestra el ejemplo

```
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. Mostrar información acerca de las LIF: `network interface show -vserver Cluster`

Muestra el ejemplo

```
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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

`network interface check cluster-connectivity start` y.. `network interface check cluster-connectivity show`

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

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
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)
```

1. Verifique que el comando de reversión automática esté habilitado en todas las LIF de clúster:

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

Muestra el ejemplo

```
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.
```

El futuro

"Instale el software NX-OS".

Instale el software NX-OS

Siga este procedimiento para instalar el software NX-OS en el switch Nexus 92300YC.

NX-OS es un sistema operativo de red para la serie Nexus de switches Ethernet y la serie MDS de switches de red de área de almacenamiento Fibre Channel (FC) proporcionados por Cisco Systems.

Revise los requisitos

Puertos y conexiones de nodo compatibles

- Los enlaces Inter-Switch (ISL) compatibles con los switches Nexus 92300YC son los puertos 1/65 y 1/66.
- Las conexiones de nodos compatibles con los switches Nexus 92300YC son los puertos 1/1 a 1/66.

Antes de empezar

Asegúrese de tener lo siguiente:

- Software Cisco NX-OS de NetApp aplicable para sus switches desde el sitio de soporte de NetApp, disponible en "mysupport.netapp.com"
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- "Página del switch Cisco Ethernet". Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.

Instale el software

Los ejemplos de este procedimiento utilizan dos nodos, pero puede tener hasta 24 nodos en un clúster.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de switch Nexus 92300YC son `cs1` y.. `cs2`.
- El ejemplo utilizado en este procedimiento inicia la actualización en el segundo interruptor, **cs2*.*
- Los nombres de LIF del clúster son `node1_clus1` y.. `node1_clus2` para los nodos 1, y. `node2_clus1` y.. `node2_clus2` para el 2.
- El nombre del espacio IP es `Cluster`.
- La `cluster1::*>` prompt indica el nombre del clúster.
- Los puertos del clúster de cada nodo se llaman `e0a` y.. `e0b`.

  Consulte "*Hardware Universe*" para los puertos de clúster reales compatibles con la plataforma.

Pasos

1. Conecte el switch de clúster a la red de gestión.
2. Utilice la `ping` Comando para verificar la conectividad con el servidor que aloja el software NX-OS y el RCF.

   Muestra el ejemplo

   Este ejemplo verifica que el switch puede llegar al servidor en la dirección IP 172.19.2.1:

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

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

3. Copie las imágenes del software NX-OS y EPLD en el switch Nexus 92300YC.

Muestra el ejemplo

```
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. Compruebe la versión que se está ejecutando del software NX-OS:

   ```
   show version
   ```

Muestra el ejemplo

```
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. Instale la imagen NX-OS.

   La instalación del archivo de imagen hace que se cargue cada vez que se reinicia el conmutador.

Muestra el ejemplo

```
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. Compruebe la nueva versión del software NX-OS una vez que se haya reiniciado el switch:

   `show version`

Muestra el ejemplo

```
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. Actualice la imagen de EPLD y reinicie el switch.

Muestra el ejemplo

```
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. Tras reiniciar el conmutador, vuelva a iniciar sesión y compruebe que la nueva versión de EPLD se ha cargado correctamente.

Muestra el ejemplo

```
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
```

El futuro

"Instale el archivo de configuración de referencia"

Instalación del archivo de configuración de referencia (RCF)

Puede instalar el RCF después de configurar el conmutador Nexus 92300YC por primera vez. También puede utilizar este procedimiento para actualizar la versión de RCF.

Consulte el artículo de la base de conocimientos "Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"para obtener más información al instalar o actualizar su RCF.

Acerca de esta tarea

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches Cisco son `cs1` y.. `cs2`.
- Los nombres de nodo son `node1` y.. `node2`.
- Los nombres de LIF del clúster son `node1_clus1`, `node1_clus2`, `node2_clus1`, y. `node2_clus2`.
- La `cluster1::*>` prompt indica el nombre del clúster.

- El procedimiento requiere el uso de tanto comandos de la ONTAP como de "Switches Cisco Nexus serie 9000"; Los comandos ONTAP se utilizan a menos que se indique lo contrario.
- Antes de realizar este procedimiento, asegúrese de que tiene una copia de seguridad actual de la configuración del conmutador.
- Durante este procedimiento no se necesita ningún enlace entre switches (ISL) operativo. Esto se debe a que los cambios en la versión de RCF pueden afectar temporalmente a la conectividad ISL. Para garantizar operaciones de clúster no disruptivas, el siguiente procedimiento migra todas las LIF del clúster al switch de partner operativo mientras realiza los pasos del switch de destino.

Pasos

1. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster: `network device-discovery show`

   Muestra el ejemplo

```
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. Compruebe el estado administrativo y operativo de cada puerto del clúster.

   a. Compruebe que todos los puertos del clúster tengan el estado correcto: `network port show -ipspace Cluster`

Muestra el ejemplo

```
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. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio: `network interface show -vserver Cluster`

Muestra el ejemplo

```
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. Compruebe que el clúster muestra información de ambos switches de clúster: `system cluster-switch show -is-monitoring-enabled-operational true`

Muestra el ejemplo

```
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. Deshabilite la reversión automática en las LIF del clúster.

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

4. En el switch de clúster cs2, apague los puertos conectados a los puertos del clúster de los nodos.

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

5. Comprobar que los puertos del clúster han migrado a los puertos alojados en el switch cs1 del clúster. Esto puede tardar unos segundos. `network interface show -vserver Cluster`

Muestra el ejemplo

```
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. Compruebe que el clúster esté en buen estado: `cluster show`

Muestra el ejemplo

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

7. Si aún no lo ha hecho, guarde una copia de la configuración actual del conmutador copiando la salida del siguiente comando en un archivo de texto:

   `show running-config`

8. Limpie la configuración del interruptor cs2 y realice una configuración básica.

   Al actualizar o aplicar una nueva RCF, debe borrar los ajustes del conmutador y realizar la configuración básica. Debe estar conectado al puerto de la consola de serie del switch para volver a configurar el switch.

   a. Limpie la configuración:

Muestra el ejemplo

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

b. Reinicie el conmutador:

Muestra el ejemplo

```
(cs2)# reload

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

9. Copie el RCF en el bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en "Switches Cisco Nexus serie 9000" guías.

   En este ejemplo se muestra el uso de TFTP para copiar un RCF al bootflash del conmutador cs2:

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

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

10. Aplique el RCF descargado anteriormente al flash de inicio.

    Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en "Switches Cisco Nexus serie 9000" guías.

En este ejemplo se muestra el archivo RCF `Nexus_92300YC_RCF_v1.0.2.txt` instalación en el conmutador cs2:

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

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

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

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

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

...

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

11. Compruebe en el conmutador que el RCF se ha combinado correctamente:

```
show running-config
```

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

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

feature lacp

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

banner motd #

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

Al aplicar el RCF por primera vez, se espera el mensaje **ERROR: Error al escribir los comandos VSH** y se puede ignorar.

1. Compruebe que el archivo RCF es la versión más reciente correcta: `show running-config`

Cuando compruebe la salida para verificar que tiene el RCF correcto, asegúrese de que la siguiente información es correcta:

- El banner de RCF
- La configuración del nodo y el puerto
- Personalizaciones

  La salida varía en función de la configuración del sitio. Compruebe la configuración del puerto y consulte las notas de versión para conocer los cambios específicos del RCF que haya instalado.

2. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la "Revise las consideraciones sobre el cableado y la configuración" para obtener información detallada sobre cualquier cambio adicional necesario.
3. Después de comprobar que las versiones de RCF y los ajustes del switch son correctos, copie el archivo running-config en el archivo startup-config.

   Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en "Switches Cisco Nexus serie 9000" guías.

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

4. Reinicie el interruptor cs2. Es posible ignorar los eventos "puertos de clúster inactivos" que se informan en los nodos mientras se reinicia el switch.

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

5. Compruebe el estado de los puertos del clúster en el clúster.

   a. Compruebe que los puertos e0d están en buen estado y en todos los nodos del clúster: `network port show -ipspace Cluster`

Muestra el ejemplo

```
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. Compruebe el estado del switch del clúster (es posible que no muestre el switch cs2, ya que las LIF no son homadas en el e0d).

Muestra el ejemplo

```
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.
```

Puede observar la siguiente salida en la consola del conmutador cs1 dependiendo de la versión RCF cargada previamente en el conmutador

```
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.
```

6. En el switch de clúster cs1, apague los puertos conectados a los puertos del clúster de los nodos.

   En el ejemplo siguiente se utiliza el resultado del ejemplo de interfaz del paso 1:

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

7. Comprobar que las LIF del clúster han migrado a los puertos alojados en el switch cs2. Esto puede tardar unos segundos. `network interface show -vserver Cluster`

   Muestra el ejemplo

```
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::*>
```

8. Compruebe que el clúster esté en buen estado: `cluster show`

Muestra el ejemplo

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

9. Repita los pasos 7 a 14 en el interruptor cs1.
10. Habilite la reversión automática en las LIF del clúster.

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

11. Reinicie el interruptor cs1. Para activar las LIF de clúster y revertir a sus puertos raíz, haga lo siguiente. Es posible ignorar los eventos "puertos de clúster inactivos" que se informan en los nodos mientras se reinicia el switch.

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

12. Compruebe que los puertos del switch conectados a los puertos del clúster estén activos.

```
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) --
.
.
```

13. Compruebe que el ISL entre cs1 y cs2 funciona: `show port-channel summary`

Muestra el ejemplo

```
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#
```

14. Compruebe que las LIF del clúster han vuelto a su puerto de inicio: `network interface show -vserver Cluster`

Muestra el ejemplo

```
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::*>
```

15. Compruebe que el clúster esté en buen estado: `cluster show`

Muestra el ejemplo

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

16. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

`network interface check cluster-connectivity start` y.. `network interface check cluster-connectivity show`

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

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ -------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```
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)
```

El futuro

"Compruebe la configuración de SSH".

Compruebe su configuración SSH

Si utiliza la supervisión de estado del switch Ethernet (CSHM) y las funciones de recogida de registros, compruebe que las claves SSH y SSH estén habilitadas en los switches de clústeres.

Pasos

1. Compruebe que SSH está habilitado:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Compruebe que las claves SSH estén habilitadas:

```
show ssh key
```

Muestra el ejemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

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

Al habilitar FIPS, debe cambiar el bitcount a 256 en el conmutador mediante el comando `ssh key ecdsa 256 force`. Consulte "Configurar la seguridad de red con FIPS" para obtener más información.

El futuro

"Configure la supervisión de estado del switch".

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.