



Configurar el software

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems-switches/switch-cisco-9336c-fx2-storage/configure-software-overview-9336c-storage.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Configurar el software 1
 - Flujo de trabajo de instalación de software para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T 1
 - Configurar los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T 1
 - Prepárese para instalar o actualizar el software NX-OS y RCF. 4
 - Instale o actualice el software NX-OS 10
 - Requisitos de revisión 10
 - Instala el software 11
 - Instalar o actualizar el RCF 33
 - Descripción general de la instalación o actualización del archivo de configuración de referencia (RCF). 33
 - Instale el archivo de configuración de referencia. 35
 - Actualiza tu archivo de configuración de referencia (RCF).. . . . 46
 - Verifique su configuración SSH 55
 - Restablecer los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T a los valores predeterminados de fábrica 57

Configurar el software

Flujo de trabajo de instalación de software para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para instalar y configurar el software para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T, siga estos pasos:

1

"Configura el interruptor"

Configure los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

2

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

El software Cisco NX-OS y los archivos de configuración de referencia (RCF) deben instalarse en los conmutadores de almacenamiento Cisco 9336C-FX2 y 9336C-FX2-T.

3

"Instale o actualice el software NX-OS"

Descargue e instale o actualice el software NX-OS en los conmutadores de almacenamiento Cisco 9336C-FX2 y 9336C-FX2-T.

4

"Instalar o actualizar el RCF"

Instale o actualice el RCF después de configurar los conmutadores Cisco 9336C-FX2 y 9336C-FX2-T por primera vez. También puede utilizar este procedimiento para actualizar su versión de RCF.

5

"Verificar la configuración 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.

6

"Restablecer el interruptor a los valores predeterminados de fábrica"

Borre las configuraciones de los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

Configurar los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T

Siga este procedimiento para configurar los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T.

Antes de empezar

Asegúrese de tener lo siguiente:

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones aplicables de NX-OS y el archivo de configuración de referencia (RCF).
- Versión aplicable de NX-OS, descargada desde "[Descarga de software de Cisco](#)" página.
- Licencias aplicables, información de red y configuración, y cables.
- Terminado "[hojas de trabajo de cableado](#)" .
- Los archivos RCF de red de clúster y de red de administración de NetApp aplicables se descargaron del sitio de soporte de NetApp en "[mysupport.netapp.com](#)" . Todos los switches de red de clúster y de red de administración de Cisco vienen con la configuración predeterminada de fábrica estándar de Cisco . Estos conmutadores también tienen la versión actual del software NX-OS pero no tienen los RCF cargados.
- Documentación requerida del interruptor. Ver "[Documentación requerida](#)" Para más información.

Pasos

1. Realice una configuración inicial de los conmutadores de red del clúster.

Proporcione las respuestas pertinentes a las siguientes preguntas de configuración inicial cuando encienda el switch por primera vez. La política de seguridad de su sitio define las respuestas y los servicios que se deben habilitar.

Inmediato	Respuesta
¿Interrumpir el aprovisionamiento automático y continuar con la configuración normal? (sí/no)	Responda con sí . El valor predeterminado es no.
¿Desea implementar un estándar de contraseñas seguras? (sí/no)	Responda con sí . La respuesta predeterminada es sí.
Introduzca la contraseña de administrador.	La contraseña predeterminada es "admin"; debe crear una contraseña nueva y segura. Una contraseña débil puede ser rechazada.
¿Desea acceder al cuadro de diálogo de configuración básica? (sí/no)	Responda con sí en la configuración inicial del switch.
¿Crear otra cuenta de inicio de sesión? (sí/no)	La respuesta depende de las políticas de su sitio web sobre administradores alternativos. El valor predeterminado es no .
¿Configurar la cadena de comunidad SNMP de solo lectura? (sí/no)	Responda con no . El valor predeterminado es no.
¿Configurar la cadena de comunidad SNMP de lectura y escritura? (sí/no)	Responda con no . El valor predeterminado es no.

Inmediato	Respuesta
Introduzca el nombre del interruptor.	El nombre del interruptor está limitado a 63 caracteres alfanuméricos.
¿Continuar con la configuración de administración fuera de banda (mgmt0)? (sí/no)	Responda con sí (la opción predeterminada) a esa pregunta. En el indicador de dirección IPv4 de mgmt0, ingrese su dirección IP: ip_address.
¿Configurar la puerta de enlace predeterminada? (sí/no)	Responda con sí . En el prompt Dirección IPv4 de la puerta de enlace predeterminada: ingrese su puerta de enlace predeterminada.
¿Configurar opciones IP avanzadas? (sí/no)	Responda con no . El valor predeterminado es no.
¿Habilitar el servicio telnet? (sí/no)	Responda con no . El valor predeterminado es no.
¿Servicio SSH habilitado? (sí/no)	Responda con sí. La respuesta predeterminada es sí.  Se recomienda utilizar SSH al usar Ethernet Switch Health Monitor (CSHM) por sus funciones de recopilación de registros. También se recomienda SSHv2 para mayor seguridad.
Ingrese el tipo de clave SSH que desea generar (dsa/rsa/rsa1).	El valor predeterminado es rsa .
Ingrese el número de bits de clave (1024-2048).	Ingrese el número de bits de clave de 1024 a 2048.
¿Configurar el servidor NTP? (sí/no)	Responda con no . El valor predeterminado es no.
Configurar la capa de interfaz predeterminada (L3/L2)	Responda con L2 . El valor predeterminado es L2.
Configurar el estado predeterminado de la interfaz del puerto del switch (apagado/abierto)	Responda con noshut . El valor predeterminado es noshut.
Configurar el perfil del sistema CoPP (estricto/moderado/permisivo/denso)	Responda con estricto . El valor predeterminado es estricto.

Inmediato	Respuesta
¿Desea editar la configuración? (sí/no)	En este punto debería ver la nueva configuración. Revise y realice los cambios necesarios en la configuración que acaba de ingresar. Responda con no cuando se le solicite si está satisfecho con la configuración. Responda con sí si desea editar su configuración.
¿Usar esta configuración y guardarla? (sí/no)	Responda con sí para guardar la configuración. Esto actualiza automáticamente las imágenes de kickstart y del sistema.  Si no guarda la configuración en este paso, ninguno de los cambios tendrá efecto la próxima vez que reinicie el switch.

2. Verifique las opciones de configuración que seleccionó en la pantalla que aparece al final de la configuración y asegúrese de guardar la configuración.
3. Compruebe la versión en los conmutadores de red del clúster y, si es necesario, descargue la versión del software compatible con NetApp en los conmutadores desde ["Descarga de software de Cisco"](#) página.

¿Que sigue?

Una vez que hayas configurado tus interruptores, podrás ["Prepárese para instalar el software NX-OS y RCF"](#).

Prepárese para instalar o actualizar el software NX-OS y RCF.

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

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la siguiente nomenclatura de interruptores y nodos:

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de los nodos son cluster1-01 y cluster1-02.
- Los nombres LIF del clúster son cluster1-01_clus1 y cluster1-01_clus2 para cluster1-01 y cluster1-02_clus1 y cluster1-02_clus2 para cluster1-02.
- El `cluster1::*>` El indicador muestra el nombre del clúster.

Acerca de esta tarea

El procedimiento requiere el uso de comandos ONTAP y comandos de switches Cisco Nexus serie 9000; se utilizan comandos ONTAP a menos que se indique lo contrario.

Pasos

1. Si AutoSupport está habilitado en este clúster, suprima la creación automática de casos invocando un mensaje de AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=x h`

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



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

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

```
set -privilege advanced
```

La solicitud avanzada(*>) aparece.

3. Muestra cuántas interfaces de interconexión de clúster están configuradas en cada nodo para cada conmutador de interconexión de clúster:

```
network device-discovery show -protocol lldp
```

Mostrar ejemplo

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/lldp				
	e0a	cs1	Eth1/2	N9K-
C9336C				
	e0b	cs2	Eth1/2	N9K-
C9336C				
cluster1-01/lldp				
	e0a	cs1	Eth1/1	N9K-
C9336C				
	e0b	cs2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

4. Compruebe el estado administrativo u operativo de cada interfaz del clúster.
 - a. Mostrar los atributos del puerto de red:

```
network port show -ipSpace Cluster
```

Mostrar ejemplo

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

```
Node: cluster1-02
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-01
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
4 entries were displayed.
```

b. Mostrar información sobre los LIF:

```
network interface show -vserver Cluster
```

Mostrar ejemplo

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

Current Vserver Port	Logical Current Is Interface Home	Status Admin/Oper	Network Address/Mask	Node

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

4 entries were displayed.

5. Verifique la conectividad de las interfaces del clúster remoto:

Puedes usar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad para la conectividad del clúster y luego mostrar los detalles:

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

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

Packet				Source	Destination
Node	Date			LIF	LIF
Loss					
-----				-----	

node1					
	3/5/2024	19:21:18	-06:00	cluster1-01_clus2	cluster1-02-
clus1	none				
	3/5/2024	19:21:20	-06:00	cluster1-01_clus2	cluster1-
02_clus2	none				
node2					
	3/5/2024	19:21:18	-06:00	cluster1-02_clus2	cluster1-
01_clus1	none				
	3/5/2024	19:21:20	-06:00	cluster1-02_clus2	cluster1-
01 clus2	none				

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

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

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

```

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

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

Mostrar ejemplo

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

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

4 entries were displayed.

¿Que sigue?

Una vez que te hayas preparado para instalar el software NX-OS y RCF, podrás ["instalar o actualizar el software NX-OS"](#).

Instale o actualice el software NX-OS

Siga este procedimiento para instalar el software NX-OS en los conmutadores Nexus 9336C-FX2 y 9336C-FX2-T.

Antes de comenzar, complete el procedimiento en ["Prepárese para instalar NX-OS y RCF."](#) .

Requisitos de revisión

Antes de empezar

Asegúrate de hacer lo siguiente:

- Ejecuta el comando `show install all impact nxos bootflash:<image_name>.bin` en el switch para revisar el impacto de instalar o actualizar la nueva imagen de software NX-OS. Verifica la integridad de la imagen, revisa si son necesarios reinicios, evalúa la compatibilidad del hardware y confirma que hay suficiente espacio.
- Revisa las notas de la versión del software NX-OS de destino para ver si hay algún requisito específico.
- Verifica que tienes una copia de seguridad actual de la configuración del conmutador.
- Verifica que tienes un clúster que funciona completamente (sin errores en los registros ni problemas similares).

Documentación sugerida

- ["página del switch Ethernet de Cisco"](#)

Consulte la tabla de compatibilidad del switch para conocer las versiones compatibles de ONTAP y NX-OS.

- ["Guías de actualización y degradación de software"](#)

Consulte las guías de software y actualización correspondientes disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de los switches de Cisco .

- ["Matriz de actualización e ISSU de Cisco Nexus 9000 y 3000"](#)

Proporciona información sobre la actualización/degradación disruptiva del software Cisco NX-OS en los switches de la serie Nexus 9000, según sus versiones actuales y objetivo.

En la página, seleccione **Actualización disruptiva** y seleccione su versión actual y la versión objetivo de la lista desplegable.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la siguiente nomenclatura de interruptores y nodos:

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de los nodos son cluster1-01, cluster1-02, cluster1-03 y cluster1-04.
- Los nombres LIF del clúster son cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2, cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1 y cluster1-04_clus2.
- El `cluster1::*>` El indicador muestra el nombre del clúster.

Instala el software

El procedimiento requiere el uso de comandos ONTAP y comandos de switches Cisco Nexus serie 9000; se utilizan comandos ONTAP a menos que se indique lo contrario.

Pasos

1. Conecte el conmutador del clúster a la red de administración.
2. Utilice el comando ping para verificar la conectividad con el servidor que aloja el software NX-OS y el RCF.

Mostrar ejemplo

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

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

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

3. Muestra los puertos del clúster en cada nodo que están conectados a los conmutadores del clúster:

```
network device-discovery show
```

Mostrar ejemplo

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                Ethernet1/7      N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C-FX2
cluster1::*>
```

4. Verifique el estado administrativo y operativo de cada puerto del clúster.

a. Verifique que todos los puertos del clúster estén **activos** y en buen estado:

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

Mostrar ejemplo

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

```
Node: cluster1-01
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::*>

b. Verifique que todas las interfaces del clúster (LIF) estén en el puerto principal:

```
network interface show -vserver Cluster
```

Mostrar ejemplo

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
Home				

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			
8 entries were displayed.				
cluster1::*>				

c. Verifique que el clúster muestre información para ambos conmutadores del clúster:

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

Mostrar ejemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model                                     -----
-----
cs1                                       cluster-network     10.233.205.90      N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                       cluster-network     10.233.205.91      N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Desactive la reversión automática en los LIF del clúster. Las LIF del clúster realizan la conmutación por error al conmutador del clúster asociado y permanecen allí mientras se realiza el procedimiento de actualización en el conmutador de destino:

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

6. Copie el software NX-OS y las imágenes EPLD al conmutador Nexus 9336C-FX2.

Mostrar ejemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Verifique la versión en ejecución del software NX-OS:

```
show version
```

Mostrar ejemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.38
  NXOS: version 9.3(4)
  BIOS compile time: 05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]

Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash: 53298520 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

8. Instale la imagen NX-OS.

La instalación del archivo de imagen provoca que este se cargue cada vez que se reinicie el switch.

Mostrar ejemplo

```
cs2# install all nxos bootflash:nxos.9.3.5.bin
```

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

```
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

```
Verifying image type.  
[] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.  
[] 100% -- SUCCESS
```

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

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

Compatibility check is done:

Module	Bootable	Impact	Install-type	Reason
1	yes	Disruptive	Reset	Default upgrade is not hitless

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-
Version		Upg-Required	
1	nxos	9.3(4)	9.3(5)
yes			
1	bios	v08.37(01/28/2020):v08.23(09/23/2015)	
v08.38(05/29/2020)		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
```

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

9. Verifique la nueva versión del software NX-OS después de que el switch se haya reiniciado:

```
show version
```

Mostrar ejemplo

```
cs2# show version
```

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
```

Software

```
  BIOS: version 05.33
  NXOS: version 9.3(5)
  BIOS compile time: 09/08/2018
  NXOS image file is: bootflash:///nxos.9.3.5.bin
  NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

```
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash: 53298520 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
```

```
Reason: Reset due to upgrade
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

10. Actualice la imagen EPLD y reinicie el switch.

Mostrar 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.9.3.5.img module all
```

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.

11. Tras reiniciar el switch, vuelva a iniciar sesión y verifique que la nueva versión de EPLD se haya cargado correctamente.

Mostrar 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

12. Verifique el estado de los puertos del clúster.

- a. Verifique que los puertos del clúster estén activos y en buen estado en todos los nodos del clúster:

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

Mostrar ejemplo

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

Node: cluster1-01

Ignore

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

Node: cluster1-02

Ignore

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

Node: cluster1-03

Ignore

						Speed (Mbps)
Health	Health	Broadcast	Domain	Link	MTU	Admin/Oper
Port	IPspace					
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0b	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

b. Verifique el estado del switch desde el clúster.

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

Mostrar ejemplo

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

cluster1-01/cdp	e0a	cs1	Ethernet1/7	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/7	N9K-
C9336C-FX2				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/8	N9K-
C9336C-FX2				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/1	N9K-
C9336C-FX2				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/2	N9K-
C9336C-FX2				

```
cluster1::*> system cluster-switch show -is-monitoring-enabled  
-operational true
```

Switch Model	Type	Address	

cs1 C9336C-FX2	cluster-network	10.233.205.90	N9K-
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	N9K-

```

C9336C-FX2
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

Dependiendo de la versión de RCF previamente cargada en el switch, es posible que observe la siguiente salida en la consola del switch cs1:

```

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.

```

13. Verifique que el clúster esté en buen estado:

```
cluster show
```

Mostrar ejemplo

```

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

```

14. Repita los pasos 6 a 13 para instalar el software NX-OS en el switch cs1.

15. Verifique la conectividad de las interfaces del clúster remoto antes de habilitar la reversión automática en los LIF del clúster:

ONTAP 9.9.1 y posteriores

Puedes usar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad para la conectividad del clúster y luego mostrar los detalles:

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

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

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

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

Packet	Source	Destination
Node	Date	LIF
Loss		
-----	-----	-----
-----	-----	-----
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-
clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-
02_clus2 none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-
01_clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-
01_clus2 none		

Todas las versiones de ONTAP

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

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

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

```

1. **[[paso 16]]**Habilite la reversión automática en los LIF del clúster.

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

2. Verifique que los LIF del clúster hayan vuelto a su puerto de origen:

```
network interface show -vserver Cluster
```

Mostrar ejemplo

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0b	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0b	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		
8 entries were displayed.				
cluster1::*>				

Si alguna LIF del clúster no ha regresado a sus puertos de origen, revuértala manualmente desde el nodo local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

¿Que sigue?

Después de instalar o actualizar el software NX-OS, puede [instalar o actualizar el RCF](#) .

Instalar o actualizar el RCF

Descripción general de la instalación o actualización del archivo de configuración de referencia (RCF).

El archivo de configuración de referencia (RCF) se instala después de configurar el switch de almacenamiento Nexus 9336C-FX2 por primera vez. Actualiza tu versión RCF

cuando tienes una versión existente del archivo RCF instalado en tu conmutador.

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración de un switch de interconexión Cisco manteniendo la conectividad remota"](#) Para obtener más información sobre la instalación o actualización de su RCF.

Configuraciones RCF disponibles

La siguiente tabla describe los RCF disponibles para diferentes configuraciones. Elija el RCF aplicable a su configuración. Ver ["Switches Ethernet de Cisco"](#) Para más información.

Para obtener detalles específicos sobre el uso de puertos y VLAN, consulte la sección de notas importantes y el banner en su RCF.

Nombre RCF	Descripción
Ruptura de alta disponibilidad de 2 clústeres	Admite dos clústeres ONTAP con al menos ocho nodos, incluidos los nodos que utilizan puertos Cluster+HA compartidos.
Ruptura de 4 clústeres HA	Admite cuatro clústeres ONTAP con al menos cuatro nodos, incluidos los nodos que utilizan puertos Cluster+HA compartidos.
1-Cluster-HA	Todos los puertos están configurados para 40/100GbE. Admite tráfico compartido de clúster/HA en puertos. Requerido para los sistemas AFF A320, AFF A250 y FAS500f . Además, todos los puertos pueden utilizarse como puertos de clúster dedicados.
1-Clúster-HA-Ruptura	Los puertos están configurados para breakout 4x10GbE, breakout 4x25GbE (RCF 1.6+ en switches 100GbE) y 40/100GbE. Admite tráfico compartido de clúster/HA en puertos para nodos que utilizan puertos compartidos de clúster/HA: sistemas AFF A320, AFF A250 y FAS500f . Además, todos los puertos pueden utilizarse como puertos de clúster dedicados.
Almacenamiento de alta disponibilidad en clúster	Los puertos están configurados para 40/100GbE para Cluster+HA, 4x10GbE breakout para Cluster y 4x25GbE breakout para Cluster+HA, y 100GbE para cada par de almacenamiento HA.
Grupo	Dos versiones de RCF con diferentes asignaciones de puertos 4x10GbE (breakout) y puertos 40/100GbE. Se admiten todos los nodos FAS y AFF , excepto los sistemas AFF A320, AFF A250 y FAS500f .
Almacenamiento	Todos los puertos están configurados para conexiones de almacenamiento NVMe de 100 GbE.

RCF disponibles

En la siguiente tabla se enumeran los RCF disponibles para los conmutadores 9336C-FX2 y 9336C-FX2-T. Elija la versión RCF aplicable para su configuración. Ver ["Switches Ethernet de Cisco"](#) Para más información.

Nombre RCF
RCF de ruptura de clúster HA 1.xx
RCF de almacenamiento de alta disponibilidad en clúster 1.xx
Almacenamiento RCF 1.xx
RCF de alta disponibilidad multiclúster 1.xx

Documentación sugerida

- ["Switches Ethernet de Cisco"](#)

Consulte la tabla de compatibilidad de switches para conocer las versiones compatibles de ONTAP y RCF en el sitio de soporte de NetApp . Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis de comandos en RCF y la sintaxis que se encuentra en versiones específicas de NX-OS.

- ["Switches Cisco Nexus serie 9000"](#)

Consulte las guías de software y actualización correspondientes disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de los switches de Cisco .

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la siguiente nomenclatura de interruptores y nodos:

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de los nodos son node1-01, node1-02, node1-03 y node1-04.
- Los nombres del clúster LIF son node1-01_clus1, node1-01_clus2, node1-02_clus1, node1-02_clus2, node1-03_clus1, node1-03_clus2, node1-04_clus1 y node1-04_clus2.
- El `cluster1::*>` El indicador muestra el nombre del clúster.

Ver el ["Hardware Universe"](#) para verificar los puertos correctos en su plataforma.



Los resultados del comando pueden variar dependiendo de las diferentes versiones de ONTAP.

Comandos utilizados

El procedimiento requiere el uso de comandos ONTAP y comandos de switches Cisco Nexus serie 9000; se utilizan comandos ONTAP a menos que se indique lo contrario.

¿Que sigue?

Después de revisar el procedimiento de instalación o actualización de RCF, puede ["instalar el RCF"](#) o ["Mejora tu RCF"](#) según sea necesario.

Instale el archivo de configuración de referencia

Debe instalar el archivo de configuración de referencia (RCF) después de configurar los conmutadores de almacenamiento Nexus 9336C-FX2 y 9336C-FX2-T por primera vez.

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración de un switch de interconexión Cisco manteniendo la conectividad remota"](#) Para obtener más información sobre la instalación de su RCF.

Antes de empezar

Verifique las siguientes instalaciones y conexiones:

- Una conexión de consola al conmutador. La conexión a la consola es opcional si tiene acceso remoto al switch.
- Los switches cs1 y cs2 están encendidos y la configuración inicial del switch está completa (la dirección IP de administración y SSH están configuradas).
- Se ha instalado la versión deseada de NX-OS.
- Los puertos del clúster de nodos ONTAP no están conectados.

Paso 1: Instale el RCF en los interruptores

1. Inicie sesión para cambiar cs1 usando SSH o mediante una consola serial.
2. Copie el RCF al bootflash del conmutador cs1 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP.

Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos de Cisco Nexus serie 9000 NX-OS"](#) .

Mostrar ejemplo

Este ejemplo muestra cómo se utiliza TFTP para copiar un RCF a la memoria flash de arranque del switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Storage.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

3. Aplique el RCF descargado previamente a la memoria flash de arranque.

Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos de Cisco Nexus serie 9000 NX-OS"](#) .

Mostrar ejemplo

Este ejemplo muestra el RCF Nexus_9336C_RCF_v1.6-Storage.txt Instalando en el switch cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-
commands
```

4. Examine la salida del banner de `show banner motd dominio`. Debe leer y seguir estas instrucciones para garantizar la correcta configuración y funcionamiento del interruptor.

Mostrar ejemplo

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Storage.txt
* Date       : 10-23-2020
* Version    : v1.6
*
* Port Usage : Storage configuration
* Ports 1-36: 100GbE Controller and Shelf Storage Ports
*****
*****
```

5. Verifique que RCF sea la versión más reciente correcta:

```
show running-config
```

Al comprobar la salida para verificar que tiene el RCF correcto, asegúrese de que la siguiente información sea correcta:

- El estandarte de RCF
- Configuración del nodo y del puerto
- Personalizaciones

El resultado varía según la configuración de su sitio. Compruebe la configuración del puerto y consulte las notas de la versión para conocer los cambios específicos del RCF que haya instalado.

6. Registre cualquier adición personalizada entre el actual `running-config` archivo y el archivo RCF en uso.
7. Después de verificar que las versiones de RCF y la configuración del interruptor sean correctas, copie el `running-config` archivo al `startup-config` archivo.

```
cs1# copy running-config startup-config
[#####] 100% Copy complete
```

8. Guarde los detalles de configuración básicos en el `write_erase.cfg` archivo en la memoria flash de arranque.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. Al instalar RCF versión 1.12 o posterior, ejecute los siguientes comandos:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración de un switch de interconexión Cisco manteniendo la conectividad remota"](#) Para obtener más detalles.

10. Verifique que el `write_erase.cfg` El archivo se ha rellenado según lo previsto:

```
show file bootflash:write_erase.cfg
```

11. Emitir el `write erase` comando para borrar la configuración guardada actual:

```
cs1# write erase

Warning: This command will erase the startup-configuration.

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

12. Copie la configuración básica guardada previamente en la configuración de inicio.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

13. Reiniciar interruptor cs1.

```
cs1# reload

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

14. Repita los pasos 1 al 13 en el interruptor cs2.

15. Conecte los puertos del clúster de todos los nodos del clúster ONTAP a los conmutadores cs1 y cs2.

Paso 2: Verifique las conexiones del interruptor

1. Verifique que los puertos del switch conectados a los puertos del clúster estén **activos**.

```
show interface brief
```

Mostrar ejemplo

```
cs1# show interface brief | grep up
mgmt0  --          up      <mgmt ip address>
1000    1500
Eth1/11      1      eth  trunk  up      none
100G(D)  --
Eth1/12      1      eth  trunk  up      none
100G(D)  --
Eth1/13      1      eth  trunk  up      none
100G(D)  --
Eth1/14      1      eth  trunk  up      none
100G(D)  --
Eth1/15      1      eth  trunk  up      none
100G(D)  --
Eth1/16      1      eth  trunk  up      none
100G(D)  --
Eth1/17      1      eth  trunk  up      none
100G(D)  --
Eth1/18      1      eth  trunk  up      none
100G(D)  --
Eth1/23      1      eth  trunk  up      none
100G(D)  --
Eth1/24      1      eth  trunk  up      none
100G(D)  --
Eth1/25      1      eth  trunk  up      none
100G(D)  --
Eth1/26      1      eth  trunk  up      none
100G(D)  --
Eth1/27      1      eth  trunk  up      none
100G(D)  --
Eth1/28      1      eth  trunk  up      none
100G(D)  --
Eth1/29      1      eth  trunk  up      none
100G(D)  --
Eth1/30      1      eth  trunk  up      none
100G(D)  --
```

2. Verifique que los nodos del clúster se encuentren en sus VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Mostrar ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Po999
30	VLAN0030	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9, Eth1/10, Eth1/11 Eth1/12, Eth1/13, Eth1/14 Eth1/15, Eth1/16, Eth1/17 Eth1/18, Eth1/19, Eth1/20 Eth1/21, Eth1/22, Eth1/23 Eth1/24, Eth1/25, Eth1/26 Eth1/27, Eth1/28, Eth1/29 Eth1/30, Eth1/31, Eth1/32 Eth1/33, Eth1/34, Eth1/35 Eth1/36

```
cs1# show interface trunk
```

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--

Eth1/9	1	trunking	--
Eth1/10	1	trunking	--
Eth1/11	1	trunking	--
Eth1/12	1	trunking	--
Eth1/13	1	trunking	--
Eth1/14	1	trunking	--
Eth1/15	1	trunking	--
Eth1/16	1	trunking	--
Eth1/17	1	trunking	--
Eth1/18	1	trunking	--
Eth1/19	1	trunking	--
Eth1/20	1	trunking	--
Eth1/21	1	trunking	--
Eth1/22	1	trunking	--
Eth1/23	1	trunking	--
Eth1/24	1	trunking	--
Eth1/25	1	trunking	--
Eth1/26	1	trunking	--
Eth1/27	1	trunking	--
Eth1/28	1	trunking	--
Eth1/29	1	trunking	--
Eth1/30	1	trunking	--
Eth1/31	1	trunking	--
Eth1/32	1	trunking	--
Eth1/33	1	trunking	--
Eth1/34	1	trunking	--
Eth1/35	1	trunking	--
Eth1/36	1	trunking	--

Port	Vlans Allowed on Trunk
------	------------------------

Eth1/1	30
Eth1/2	30
Eth1/3	30
Eth1/4	30
Eth1/5	30
Eth1/6	30
Eth1/7	30
Eth1/8	30
Eth1/9	30
Eth1/10	30
Eth1/11	30
Eth1/12	30

Eth1/13	30
Eth1/14	30
Eth1/15	30
Eth1/16	30
Eth1/17	30
Eth1/18	30
Eth1/19	30
Eth1/20	30
Eth1/21	30
Eth1/22	30
Eth1/23	30
Eth1/24	30
Eth1/25	30
Eth1/26	30
Eth1/27	30
Eth1/28	30
Eth1/29	30
Eth1/30	30
Eth1/31	30
Eth1/32	30
Eth1/33	30
Eth1/34	30
Eth1/35	30
Eth1/36	30

Port	Vlans Err-disabled on Trunk
------	-----------------------------

Eth1/1	none
Eth1/2	none
Eth1/3	none
Eth1/4	none
Eth1/5	none
Eth1/6	none
Eth1/7	none
Eth1/8	none
Eth1/9	none
Eth1/10	none
Eth1/11	none
Eth1/12	none
Eth1/13	none
Eth1/14	none
Eth1/15	none
Eth1/16	none

Eth1/17	none
Eth1/18	none
Eth1/19	none
Eth1/20	none
Eth1/21	none
Eth1/22	none
Eth1/23	none
Eth1/24	none
Eth1/25	none
Eth1/26	none
Eth1/27	none
Eth1/28	none
Eth1/29	none
Eth1/30	none
Eth1/31	none
Eth1/32	none
Eth1/33	none
Eth1/34	none
Eth1/35	none
Eth1/36	none

Port	STP Forwarding
------	----------------

Eth1/1	none
Eth1/2	none
Eth1/3	none
Eth1/4	none
Eth1/5	none
Eth1/6	none
Eth1/7	none
Eth1/8	none
Eth1/9	none
Eth1/10	none
Eth1/11	30
Eth1/12	30
Eth1/13	30
Eth1/14	30
Eth1/15	30
Eth1/16	30
Eth1/17	30
Eth1/18	30
Eth1/19	none
Eth1/20	none

Eth1/21	none
Eth1/22	none
Eth1/23	30
Eth1/24	30
Eth1/25	30
Eth1/26	30
Eth1/27	30
Eth1/28	30
Eth1/29	30
Eth1/30	30
Eth1/31	none
Eth1/32	none
Eth1/33	none
Eth1/34	none
Eth1/35	none
Eth1/36	none

Port	Vlans in spanning tree forwarding state and not pruned

Eth1/1	Feature VTP is not enabled
none	
Eth1/2	Feature VTP is not enabled
none	
Eth1/3	Feature VTP is not enabled
none	
Eth1/4	Feature VTP is not enabled
none	
Eth1/5	Feature VTP is not enabled
none	
Eth1/6	Feature VTP is not enabled
none	
Eth1/7	Feature VTP is not enabled
none	
Eth1/8	Feature VTP is not enabled
none	
Eth1/9	Feature VTP is not enabled
none	
Eth1/10	Feature VTP is not enabled
none	
Eth1/11	Feature VTP is not enabled
30	
Eth1/12	Feature VTP is not enabled
30	

Eth1/13	Feature VTP is not enabled
30	
Eth1/14	Feature VTP is not enabled
30	
Eth1/15	Feature VTP is not enabled
30	
Eth1/16	Feature VTP is not enabled
30	
Eth1/17	Feature VTP is not enabled
30	
Eth1/18	Feature VTP is not enabled
30	
Eth1/19	Feature VTP is not enabled
none	
Eth1/20	Feature VTP is not enabled
none	
Eth1/21	Feature VTP is not enabled
none	
Eth1/22	Feature VTP is not enabled
none	
Eth1/23	Feature VTP is not enabled
30	
Eth1/24	Feature VTP is not enabled
30	
Eth1/25	Feature VTP is not enabled
30	
Eth1/26	Feature VTP is not enabled
30	
Eth1/27	Feature VTP is not enabled
30	
Eth1/28	Feature VTP is not enabled
30	
Eth1/29	Feature VTP is not enabled
30	
Eth1/30	Feature VTP is not enabled
30	
Eth1/31	Feature VTP is not enabled
none	
Eth1/32	Feature VTP is not enabled
none	
Eth1/33	Feature VTP is not enabled
none	
Eth1/34	Feature VTP is not enabled
none	
Eth1/35	Feature VTP is not enabled
none	

```
Eth1/36      Feature VTP is not enabled
none
```



Para obtener detalles específicos sobre el uso de puertos y VLAN, consulte la sección de notas importantes y el banner en su RCF.

Paso 3: Configura tu clúster ONTAP

NetApp recomienda utilizar System Manager para configurar nuevos clústeres.

System Manager proporciona un flujo de trabajo simple y fácil para la configuración del clúster, incluyendo la asignación de una dirección IP de administración de nodos, la inicialización del clúster, la creación de una capa local, la configuración de protocolos y el aprovisionamiento de almacenamiento inicial.

Ir a ["Configurar ONTAP en un nuevo clúster con el Administrador del sistema"](#) Para obtener instrucciones de configuración.

¿Que sigue?

Una vez instalado el RCF, puedes ["verificar la configuración de SSH"](#)

Actualiza tu archivo de configuración de referencia (RCF).

Actualizas tu versión de RCF cuando tienes una versión existente del archivo RCF instalada en tus switches operativos.

Antes de empezar

Asegúrese de tener lo siguiente:

- Una copia de seguridad actualizada de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros ni problemas similares).
- El RCF actual.
- Si está actualizando su versión de RCF, necesita una configuración de arranque en RCF que refleje las imágenes de arranque deseadas.

Si necesita cambiar la configuración de arranque para que refleje las imágenes de arranque actuales, debe hacerlo antes de volver a aplicar el RCF para que se instancie la versión correcta en futuros reinicios.



No se necesita ningún enlace entre conmutadores (ISL) operativo durante este procedimiento. Esto es así por diseño porque los cambios de versión de RCF pueden afectar la conectividad de ISL temporalmente. Para garantizar un funcionamiento ininterrumpido del clúster, el siguiente procedimiento migra todas las LIF del clúster al conmutador asociado operativo mientras se realizan los pasos en el conmutador de destino.



Antes de instalar una nueva versión del software del switch y los RCF, debe borrar la configuración del switch y realizar una configuración básica. Debe estar conectado al switch mediante la consola serie o haber guardado la información de configuración básica antes de borrar la configuración del switch.

Paso 1: Prepárese para la actualización

1. Si AutoSupport está habilitado en este clúster, suprima 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.

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

```
set -privilege advanced
```

Aparece el indicador avanzado (*>).

3. Muestra los puertos en cada nodo que están conectados a los conmutadores:

```
network device-discovery show
```

Mostrar ejemplo

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID) Interface      Platform
-----
node1-01/cdp
           e3a    cs1                Ethernet1/7    N9K-
C9336C
           e3b    cs2                Ethernet1/7    N9K-
C9336C
node1-02/cdp
           e3a    cs1                Ethernet1/8    N9K-
C9336C
           e3b    cs2                Ethernet1/8    N9K-
C9336C
.
.
.
```

4. Verifique que todos los puertos de almacenamiento se encuentren en buen estado:

```
storage port show -port-type ENET
```

Mostrar ejemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
node1-02						
	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
.						
.						
.						

5. Desactive la reversión automática en los LIF del clúster.

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

Paso 2: Configurar puertos

1. En el conmutador cs1, apague los puertos conectados a todos los puertos de los nodos.

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



Asegúrese de apagar **todos** los puertos conectados para evitar problemas de conexión de red. Consulte el artículo de la base de conocimientos ["Nodo fuera de quórum al migrar la LIF del clúster durante la actualización del sistema operativo del switch"](#) Para obtener más detalles.

2. Verifique que los LIF del clúster hayan conmutado por error a los puertos alojados en el conmutador cs1. Esto podría tardar unos segundos.

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

Mostrar ejemplo

```
cluster1::*> network interface show -role cluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e7a	node1-01_clus1	up/up	169.254.36.44/16	node1-01
e7b	node1-01_clus2	up/up	169.254.7.5/16	node1-01
e7a	node1-02_clus1	up/up	169.254.197.206/16	node1-02
e7b	node1-02_clus2	up/up	169.254.195.186/16	node1-02
e7a	node1-03_clus1	up/up	169.254.192.49/16	node1-03
e7b	node1-03_clus2	up/up	169.254.182.76/16	node1-03
e7a	node1-04_clus1	up/up	169.254.59.49/16	node1-04
e7b	node1-04_clus2	up/up	169.254.62.244/16	node1-04

8 entries were displayed.

3. Verifique que el clúster esté en buen estado:

```
cluster show
```

Mostrar ejemplo

```
cluster1::*> cluster show
Node           Health Eligibility  Epsilon
-----
node1-01       true   true        false
node1-02       true   true        false
node1-03       true   true         true
node1-04       true   true        false

4 entries were displayed.
```

4. Si aún no lo ha hecho, guarde una copia de la configuración actual del switch copiando el resultado del siguiente comando en un archivo de texto:

```
show running-config
```

- Registre cualquier adición personalizada entre el actual `running-config` y el archivo RCF en uso (como una configuración SNMP para su organización).
 - Para NX-OS 10.2 y versiones posteriores, utilice el `show diff running-config` comando para comparar con el archivo RCF guardado en la memoria flash de arranque. De lo contrario, utilice una herramienta de comparación o diff de terceros.
5. Guarde los detalles de configuración básicos en el `write_erase.cfg` archivo en la memoria flash de arranque.



Asegúrese de configurar lo siguiente:

- Nombre de usuario y contraseña
- Dirección IP de gestión
- Puerta de enlace predeterminada
- Cambiar nombre

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg
```

```
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

6. Al actualizar a la versión 1.12 de RCF o posterior, ejecute los siguientes comandos: `cs1# echo "hardware access-list tcam region ing-racl 1024" >> bootflash:write_erase.cfg`

```
cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region ing-l2-qos 1280 >>
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración de un switch de interconexión Cisco manteniendo la conectividad remota"](#) Para obtener más detalles.

7. Verifique que el `write_erase.cfg` El archivo se ha rellenado según lo previsto:

```
show file bootflash:write_erase.cfg
```

8. Emitir el `write erase` comando para borrar la configuración guardada actual:

```
cs1# write erase
```

Warning: This command will erase the startup-configuration.

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

9. Copie la configuración básica guardada previamente en la configuración de inicio.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Reinicia el switch:

```
cs1# reload
```

This command will reboot the system. (y/n)? [n] **y**

11. Una vez que la dirección IP de administración vuelva a ser accesible, inicie sesión en el switch a través de SSH.

Es posible que necesites actualizar las entradas del archivo host relacionadas con las claves SSH.

12. Copie el RCF al bootflash del conmutador cs1 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP.

Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos de Cisco Nexus serie 9000 NX-OS"](#) guías.

Mostrar ejemplo

Este ejemplo muestra cómo se utiliza TFTP para copiar un RCF a la memoria flash de arranque del switch cs1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Storage.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

13. Aplique el RCF descargado previamente a la memoria flash de arranque.

Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos de Cisco Nexus serie 9000 NX-OS"](#) guías.

Este ejemplo muestra el archivo RCF. NX9336C-FX2-RCF-v1.13-1-Storage.txt Instalando en el switch cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-commands
```



Asegúrese de leer detenidamente las secciones **Notas de instalación**, **Notas importantes** y **banner** de su RCF. Debe leer y seguir estas instrucciones para garantizar la configuración y el funcionamiento adecuados del conmutador.

14. Verifique que el archivo RCF sea la versión más reciente correcta:

```
show running-config
```

Al comprobar la salida para verificar que tiene el RCF correcto, asegúrese de que la siguiente información sea correcta:

- El estandarte de RCF
- Configuración del nodo y del puerto
- Personalizaciones

El resultado varía según la configuración de su sitio. Compruebe la configuración del puerto y consulte las notas de la versión para conocer los cambios específicos del RCF que haya instalado.

15. Vuelva a aplicar cualquier personalización anterior a la configuración del switch.
16. Después de verificar que las versiones de RCF, las adiciones personalizadas y la configuración del interruptor sean correctas, copie el running-config archivo al startup-config archivo.

Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos de Cisco Nexus serie 9000 NX-OS"](#) guías.

```
cs1# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

17. Reiniciar interruptor cs1. Puede ignorar las alertas de "monitor de estado del conmutador de clúster" y los eventos de "puertos de clúster inactivos" que se informan en los nodos mientras se reinicia el conmutador.

```
cs1# reload
```

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

18. Verifique que todos los puertos de almacenamiento se encuentren en buen estado:

```
storage port show -port-type ENET
```

Mostrar ejemplo

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status

node1-01						
	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
node1-02						
	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
.						
.						
.						

19. Verifique que el clúster esté en buen estado:

```
cluster show
```

Mostrar ejemplo

```
cluster1::*> cluster show
Node           Health  Eligibility  Epsilon
-----
node1-01       true    true         false
node1-02       true    true         false
node1-03       true    true         true
node1-04       true    true         false

4 entries were displayed.
```

20. Repita los pasos 4 a 19 en el interruptor cs2.
21. Habilitar la reversión automática en los LIF del clúster.

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

Paso 3: Verifique la configuración de red y el estado del clúster.

1. Verifique que los puertos del switch conectados a los puertos del clúster estén **activos**.

```
show interface brief
```

2. Verifique que los nodos esperados sigan conectados:

```
show cdp neighbors
```

3. Verifique que los nodos del clúster se encuentren en sus VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

4. Verifique que los LIF del clúster hayan vuelto a su puerto de origen:

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

Si alguna LIF del clúster no ha regresado a sus puertos de origen, reviértala manualmente desde el nodo local:

```
network interface revert -vserver vserver_name -lif <lif-name>
```

5. Verifique que el clúster esté en buen estado:

```
cluster show
```

6. Verifique la conectividad de las interfaces del clúster remoto:

- a. Puedes usar el `network interface check cluster-connectivity show` comando para mostrar los detalles de una comprobación de accesibilidad para la conectividad del clúster:

```
network interface check cluster-connectivity show
```

- b. Alternativamente, puede utilizar el `cluster ping-cluster -node <node-name>` comando para comprobar la conectividad:

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

¿Que sigue?

Después de actualizar tu RCF, puedes ["verificar la configuración de SSH"](#) .

Verifique su configuración SSH

Si está utilizando las funciones de monitorización del estado del conmutador Ethernet (CSHM) y recopilación de registros, verifique que SSH y las claves SSH estén habilitadas en los conmutadores del clúster.

Pasos

1. Verifique que SSH esté habilitado:

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

2. Verifique que las claves SSH estén habilitadas:

```
show ssh key
```

Mostrar ejemplo

```
(switch)# show ssh key

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

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

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



Al habilitar FIPS, debe cambiar el recuento de bits a 256 en el conmutador mediante el comando `ssh key ecdsa 256 force`. Ver ["Configure la seguridad de la red utilizando FIPS."](#) Para obtener más detalles.

¿Que sigue?

Después de verificar tu configuración SSH, ["configurar la monitorización del estado del conmutador"](#).

Restablecer los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T a los valores predeterminados de fábrica

Para restablecer los interruptores de almacenamiento 9336C-FX2 y 9336C-FX2-T a los valores predeterminados de fábrica, debe borrar las configuraciones de los interruptores 9336C-FX2 y 9336C-FX2-T.

Acerca de esta tarea

- Debes estar conectado al switch mediante la consola serie.
- Esta tarea restablece la configuración de la red de administración.

Pasos

1. Borrar la configuración existente:

```
write erase
```

```
(cs2)# write erase
```

```
Warning: This command will erase the startup-configuration.  
Do you wish to proceed anyway? (y/n) [n] y
```

2. Recargue el software del conmutador:

```
reload
```

```
(cs2)# reload
```

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

El sistema se reinicia y entra en el asistente de configuración. Durante el arranque, si recibe el mensaje “¿Desea cancelar el aprovisionamiento automático y continuar con la configuración normal?” (sí/no)[n]”, debe responder **sí** para continuar.

¿Qué sigue?

Después de reiniciar los interruptores, puedes [reconfigurar](#) los que necesiten.

Información de copyright

Copyright © 2026 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.