



Commutadores de almacenamiento

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-switch-overview-9336c-storage.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Comutadores de almacenamiento	1
Cisco Nexus 9336C-FX2 o 9336C-FX2-T	1
Empezar	1
Instala el hardware	6
Configurar el software	17
Reemplace los comutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T	74
Cisco Nexus 3232C	80
Empezar	80
Instalar hardware	84
Configurar software	89
Reemplazar un switch de almacenamiento Cisco Nexus 3232C	127
Actualizar un switch de almacenamiento Cisco Nexus 3232C	134
NVIDIA SN2100	149
Empezar	149
Instalar hardware	151
Configurar software	161
Migrar interruptores	193
Reemplazar un comutador de almacenamiento NVIDIA SN2100	203

Comutadores de almacenamiento

Cisco Nexus 9336C-FX2 o 9336C-FX2-T

Empezar

Flujo de trabajo de instalación y configuración para los comutadores de almacenamiento Cisco Nexus 9336C-FX2 9336C-FX2-T

Los comutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T son parte de la plataforma Cisco Nexus 9000 y se pueden instalar en un gabinete de sistema NetApp .

Cisco Nexus 9336C-FX2 (36 puertos) es un comutador de datos/almacenamiento/clúster de alta densidad de puertos. Cisco Nexus 9336C-FX2-T (12 puertos) es un comutador de alto rendimiento y baja densidad de puertos que admite configuraciones 10/25/40/100 GbE.

Siga estos pasos de flujo de trabajo para instalar y configurar sus comutadores Cisco 9336C-FX2 y 9336C-FX2-T.

1

"Revisar los requisitos de configuración"

Revise los requisitos de configuración para los comutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

2

"Revise los componentes y números de pieza"

Revise los componentes y números de pieza de los comutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

3

"Revisar la documentación requerida"

Revise la documentación específica del comutador y del controlador para configurar los comutadores 9336C-FX2 y 9336C-FX2-T y el clúster ONTAP .

4

"Revisar los requisitos de Smart Call Home"

Revise los requisitos de la función Cisco Smart Call Home, que se utiliza para monitorear los componentes de hardware y software de su red.

5

"Instala el hardware"

Instale el hardware del interruptor.

6

"Configurar el software"

Configurar el software del comutador.

Requisitos de configuración para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para la instalación y el mantenimiento de los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T, asegúrese de revisar la configuración y los requisitos de red.

Compatibilidad con ONTAP

ONTAP 9.9.1 y posteriores

A partir de ONTAP 9.9.1, puede utilizar los switches Cisco Nexus 9336C-FX2 para combinar la funcionalidad de almacenamiento y clúster en una configuración de switch compartido.

Si desea crear clústeres ONTAP con más de dos nodos, necesitará dos conmutadores de red compatibles.



El monitor de estado del switch Ethernet no es compatible con ONTAP 9.13.1P8 y versiones anteriores ni con 9.14.1P3 y versiones anteriores ni con NX-OS versión 10.3(4a)(M).

ONTAP 9.10.1 y posteriores

Además, a partir de ONTAP 9.10.1, puede utilizar los conmutadores Cisco Nexus 9336C-FX2-T para combinar la funcionalidad de almacenamiento y clúster en una configuración de conmutador compartido.

Si desea crear clústeres ONTAP con más de dos nodos, necesitará dos conmutadores de red compatibles.

Requisitos de configuración

Para la configuración, necesitará el número y tipo adecuados de cables y conectores de cable para sus conmutadores.

Dependiendo del tipo de switch que esté configurando inicialmente, deberá conectarse al puerto de consola del switch con el cable de consola incluido; también deberá proporcionar información de red específica.

Requisitos de red

Necesita la siguiente información de red para todas las configuraciones del conmutador.

- Subred IP para la gestión del tráfico de red
- Nombres de host y direcciones IP para cada uno de los controladores del sistema de almacenamiento y todos los conmutadores aplicables
- La mayoría de los controladores del sistema de almacenamiento se administran a través de la interfaz e0M conectándose al puerto de servicio Ethernet (ícono de llave inglesa). En los sistemas AFF A800 y AFF A700s , la interfaz e0M utiliza un puerto Ethernet dedicado.
- Consulte el "[Hardware Universe](#)" Para obtener la información más reciente.

Para obtener más información sobre la configuración inicial de su switch, consulte la siguiente guía: "[Guía de instalación y actualización de Cisco Nexus 9336C-FX2](#)" .

¿Qué sigue?

Después de revisar los requisitos de configuración, puede confirmar su "[componentes y números de pieza](#)".

Componentes y números de pieza para los switches de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para la instalación y el mantenimiento de los switches de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T, asegúrese de revisar la lista de componentes y números de pieza.

La siguiente tabla enumera el número de pieza y la descripción de los conmutadores de almacenamiento, ventiladores y fuentes de alimentación 9336C-FX2 y 9336C-FX2-T:

Número de pieza	Descripción
X190200-CS-PE	Conmutador de clúster, N9336C 36Pt PTSX 10/25/40/100G
X190200-CS-PI	Conmutador de clúster, N9336C 36Pt PSIN 10/25/40/100G
X190212-CS-PE	Conmutador de clúster, N9336C 12Pt (9336C-FX2-T) PTSX 10/25/40/100G
X190212-CS-PI	Conmutador de clúster, N9336C 12Pt (9336C-FX2-T) PSIN 10/25/40/100G
SW-N9K-FX2-24P-UPG	Licencia de software Cisco 9336CFX2 para POD de 24 puertos
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100GQSFP28
X190002	Kit de accesorios X190001/X190003
X-NXA-PAC-1100W-PE2	Fuente de alimentación N9K-9336C AC 1100W - Flujo de aire de escape del lado del puerto
X-NXA-PAC-1100W-PI2	Fuente de alimentación N9K-9336C AC 1100W - Entrada de aire por el lado del puerto
X-NXA-FAN-65CFM-PE	N9K-9336C 65 CFM, flujo de aire de escape del lado de babor
X-NXA-FAN-65CFM-PI	N9K-9336C 65 CFM, flujo de aire de entrada del lado de babor

Licencias inteligentes de Cisco solo para puertos 9336C-FX2-T

Para activar más de 12 puertos en su switch de almacenamiento Cisco Nexus 9336C-FX-T, debe adquirir una licencia Cisco Smart. Las licencias Cisco Smart se gestionan a través de cuentas Cisco Smart.

1. Cree una nueva cuenta Smart, si es necesario. Ver "[Crea una nueva cuenta inteligente](#)" Para más detalles.
2. Solicitar acceso a una cuenta Smart existente. Ver "[Solicitar acceso a una cuenta Smart existente](#)" Para más detalles.



Una vez que haya adquirido su licencia Smart, instale el RCF apropiado para habilitar y configurar los 36 puertos disponibles para su uso.

¿Qué sigue?

Una vez que haya confirmado sus componentes y números de pieza, puede revisar el "["documentación requerida"](#)".

Requisitos de documentación para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para la instalación y el mantenimiento de los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T, asegúrese de revisar la documentación específica del conmutador y del controlador para configurar los conmutadores Cisco 9336-FX2 y el clúster ONTAP .

Documentación del interruptor

Para configurar los switches Cisco Nexus 9336C-FX2, necesita la siguiente documentación de "["Soporte para switches Cisco Nexus serie 9000"](#)" página:

Título del documento	Descripción
<i>Guía de instalación de hardware de la serie Nexus 9000</i>	Proporciona información detallada sobre los requisitos del sitio, detalles del hardware del switch y opciones de instalación.
<i>Guías de configuración de software para switches Cisco Nexus serie 9000</i> (elija la guía correspondiente a la versión de NX-OS instalada en sus switches)	Proporciona la información de configuración inicial del switch que necesita antes de poder configurarlo para el funcionamiento de ONTAP .
<i>Guía de actualización y degradación de software NX-OS de la serie Cisco Nexus 9000</i> (elija la guía correspondiente a la versión de NX-OS instalada en sus switches)	Proporciona información sobre cómo degradar el software del switch a uno compatible con ONTAP , si fuera necesario.
<i>Índice maestro de referencia de comandos de Cisco Nexus serie 9000 NX-OS</i>	Proporciona enlaces a las diversas referencias de comandos proporcionadas por Cisco.
<i>Referencia de MIB de Cisco Nexus 9000</i>	Describe los archivos de la Base de Información de Gestión (MIB) para los switches Nexus 9000.
<i>Referencia de mensajes del sistema NX-OS de la serie Nexus 9000</i>	Describe los mensajes del sistema para los switches Cisco Nexus serie 9000, aquellos que son informativos y otros que podrían ayudar a diagnosticar problemas con los enlaces, el hardware interno o el software del sistema.

Título del documento	Descripción
<i>Notas de la versión de NX-OS de la serie Cisco Nexus 9000 (elija las notas correspondientes a la versión de NX-OS instalada en sus switches)</i>	Describe las características, errores y limitaciones de la serie Cisco Nexus 9000.
Información sobre cumplimiento normativo y seguridad para la serie Cisco Nexus 9000	Proporciona información sobre cumplimiento normativo, seguridad y requisitos legales de organismos internacionales para los switches de la serie Nexus 9000.

Documentación de los sistemas ONTAP

Para configurar un sistema ONTAP , necesita los siguientes documentos para su versión del sistema operativo de ["ONTAP 9"](#) .

Nombre	Descripción
Instrucciones de instalación y configuración específicas del controlador	Describe cómo instalar el hardware de NetApp .
Documentación de ONTAP	Proporciona información detallada sobre todos los aspectos de las versiones de ONTAP .
"Hardware Universe"	Proporciona información sobre la configuración y compatibilidad del hardware de NetApp .

Documentación del kit de rieles y del gabinete

Para instalar un switch Cisco 9336-FX2 en un gabinete NetApp , consulte la siguiente documentación de hardware.

Nombre	Descripción
"Gabinete de sistema 42U, guía profunda"	Describe las FRU asociadas con el gabinete del sistema 42U y proporciona instrucciones de mantenimiento y reemplazo de FRU.
"Instale un switch Cisco 9336-FX2 en un gabinete NetApp"	Describe cómo instalar un switch Cisco Nexus 9336C-FX2 en un gabinete NetApp de cuatro postes.

Requisitos de Smart Call Home

Para utilizar Smart Call Home, debe configurar un conmutador de red de clúster para comunicarse mediante correo electrónico con el sistema Smart Call Home. Además, puede configurar opcionalmente su conmutador de red de clúster para aprovechar la función de soporte Smart Call Home integrada de Cisco.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Antes de poder utilizar Smart Call Home, tenga en cuenta los siguientes requisitos:

- Debe haber un servidor de correo electrónico instalado.
- El switch debe tener conectividad IP con el servidor de correo electrónico.
- Debe configurarse el nombre del contacto (contacto del servidor SNMP), el número de teléfono y la información de la dirección postal. Esto es necesario para determinar el origen de los mensajes recibidos.
- Debe asociarse un ID de CCO con un contrato de servicio Cisco SMARTnet apropiado para su empresa.
- El servicio Cisco SMARTnet debe estar instalado para que el dispositivo pueda registrarse.

El "[sitio de soporte de Cisco](#)" Contiene información sobre los comandos para configurar Smart Call Home.

Instala el hardware

Flujo de trabajo de instalación de hardware para los comutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para instalar y configurar el hardware de los comutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T, siga estos pasos:

1

"Complete la hoja de trabajo de cableado"

La hoja de cálculo de cableado de muestra proporciona ejemplos de asignaciones de puertos recomendadas desde los comutadores a los controladores. La hoja de trabajo en blanco proporciona una plantilla que puede utilizar para configurar su clúster.

2

"Instala el interruptor"

Instale los comutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

3

"Instale el switch en un armario NetApp"

Instale los comutadores 9336C-FX2 y 9336C-FX2-T y el panel de paso en un gabinete NetApp según sea necesario.

Complete la hoja de trabajo de cableado de Cisco Nexus 9336C-FX2 o 9336C-FX2-T

Si desea documentar las plataformas compatibles, descargue un PDF de esta página y complete la hoja de trabajo de cableado.

La hoja de cálculo de cableado de muestra proporciona ejemplos de asignaciones de puertos recomendadas desde los comutadores a los controladores. La hoja de trabajo en blanco proporciona una plantilla que puede

utilizar para configurar su clúster.

- [Hoja de trabajo de cableado de muestra 9336C-FX2](#)
- [Hoja de cableado en blanco 9336C-FX2](#)
- [Hoja de trabajo de cableado de muestra 9336C-FX2-T \(12 puertos\)](#)
- [Hoja de cableado en blanco 9336C-FX2-T \(12 puertos\)](#)

Hoja de trabajo de cableado de muestra 9336C-FX2

La definición de puerto de muestra en cada par de comutadores es la siguiente:

Interruptor de clúster A		Interruptor de clúster B	
Puerto de comutación	Uso de nodos y puertos	Puerto de comutación	Uso de nodos y puertos
1	4x100GbE nodo 1	1	4x100GbE nodo 1
2	4x100GbE nodo 2	2	4x100GbE nodo 2
3	4x100GbE nodo 3	3	4x100GbE nodo 3
4	4 nodos 4x100GbE	4	4 nodos 4x100GbE
5	4x100GbE nodo 5	5	4x100GbE nodo 5
6	4x100GbE nodo 6	6	4x100GbE nodo 6
7	4x100GbE nodo 7	7	4x100GbE nodo 7
8	4x100GbE nodo 8	8	4x100GbE nodo 8
9	Nodo 9 con 4x100GbE	9	Nodo 9 con 4x100GbE
10	4x100GbE nodo 10	10	4x100GbE nodo 10
11	4x100GbE nodo 11	11	4x100GbE nodo 11
12	4x100GbE nodo 12	12	4x100GbE nodo 12
13	4x100GbE nodo 13	13	4x100GbE nodo 13
14	4x100GbE nodo 14	14	4x100GbE nodo 14
15	4x100GbE nodo 15	15	4x100GbE nodo 15

Interruptor de clúster A		Interruptor de clúster B	
16	4x100GbE nodo 16	16	4x100GbE nodo 16
17	4x100GbE nodo 17	17	4x100GbE nodo 17
18	4x100GbE nodo 18	18	4x100GbE nodo 18
19	Nodo 19 con 4x100GbE	19	Nodo 19 con 4x100GbE
20	4x100GbE nodo 20	20	4x100GbE nodo 20
21	4x100GbE nodo 21	21	4x100GbE nodo 21
22	4x100GbE nodo 22	22	4x100GbE nodo 22
23	4x100GbE nodo 23	23	4x100GbE nodo 23
24	4 nodos 100GbE 24	24	4 nodos 100GbE 24
25	4x100GbE nodo 25	25	4x100GbE nodo 25
26	4x100GbE nodo 26	26	4x100GbE nodo 26
27	4x100GbE nodo 27	27	4x100GbE nodo 27
28	4x100GbE nodo 28	28	4x100GbE nodo 28
29	4x100GbE nodo 29	29	4x100GbE nodo 29
30	4x100GbE nodo 30	30	4x100GbE nodo 30
31	4x100GbE nodo 31	31	4x100GbE nodo 31
32	4x100GbE nodo 32	32	4x100GbE nodo 32
33	4x100GbE nodo 33	33	4x100GbE nodo 33
30	4x100GbE nodo 30	30	4x100GbE nodo 33
34	4x100GbE nodo 34	34	4x100GbE nodo 34
35	4x100GbE nodo 35	35	4x100GbE nodo 35
36	4x100GbE nodo 36	36	4x100GbE nodo 36

Hoja de cableado en blanco 9336C-FX2

Puede utilizar la hoja de trabajo de cableado en blanco para documentar las plataformas que se admiten como nodos en un clúster. La sección *Conexiones de clúster admitidas* de "Hardware Universe" Define los puertos del clúster utilizados por la plataforma.

Interruptor de clúster A	Interruptor de clúster B
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16
17	17
18	18
19	19

Interruptor de clúster A		Interruptor de clúster B	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	

Hoja de trabajo de cableado de muestra 9336C-FX2-T (12 puertos)

La definición de puerto de muestra en cada par de conmutadores es la siguiente:

Interruptor de clúster A		Interruptor de clúster B	
Puerto de conmutación	Uso de nodos y puertos	Puerto de conmutación	Uso de nodos y puertos
1	4x100GbE nodo 1	1	4x100GbE nodo 1

Interruptor de clúster A		Interruptor de clúster B	
2	4x100GbE nodo 2	2	4x100GbE nodo 2
3	4x100GbE nodo 3	3	4x100GbE nodo 3
4	4 nodos 4x100GbE	4	4 nodos 4x100GbE
5	4x100GbE nodo 5	5	4x100GbE nodo 5
6	4x100GbE nodo 6	6	4x100GbE nodo 6
7	4x100GbE nodo 7	7	4x100GbE nodo 7
8	4x100GbE nodo 8	8	4x100GbE nodo 8
9	Nodo 9 con 4x100GbE	9	Nodo 9 con 4x100GbE
10	4x100GbE nodo 10	10	4x100GbE nodo 10
11 a 36	Requiere licencia	11 al 36	Requiere licencia

Hoja de cableado en blanco 9336C-FX2-T (12 puertos)

Puede utilizar la hoja de trabajo de cableado en blanco para documentar las plataformas que se admiten como nodos en un clúster.

Interruptor de clúster A		Interruptor de clúster B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	

Interruptor de clúster A		Interruptor de clúster B	
10		10	
11 al 36	Requiere licencia	11 al 36	Requiere licencia

Ver el "[Hardware Universe](#)" Para obtener más información sobre los puertos del switch.

¿Qué sigue?

Una vez que hayas completado tus hojas de trabajo de cableado, podrás "[instalar el interruptor](#)".

Instalar los commutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T

Siga este procedimiento para instalar los commutadores de almacenamiento 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 de "[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 commutadores 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. Instale en rack los commutadores y controladores de la red del clúster y de la red de administración.

Si estás instalando tu...	Entonces...
Cisco Nexus 9336C-FX2 en un gabinete de sistema NetApp	Ver " Instale el switch en el armario NetApp ." Para obtener instrucciones sobre cómo instalar el switch en un armario NetApp .
Equipos en un rack de telecomunicaciones	Consulte los procedimientos proporcionados en las guías de instalación del hardware del switch y las instrucciones de instalación y configuración de NetApp .

2. Conecte los commutadores de red del clúster y de la red de administración a los controladores utilizando las hojas de trabajo de cableado completadas.
3. Encienda la alimentación de los commutadores y controladores de la red del clúster y de la red de administración.

¿Qué sigue?

Opcionalmente, puedes ["Instalar un conmutador Cisco Nexus 9336C-FX2 en un gabinete NetApp"](#). De lo contrario, vaya a ["configurar el conmutador"](#).

Instalar los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T en un gabinete NetApp

Dependiendo de su configuración, es posible que necesite instalar los conmutadores Cisco Nexus 9336C-FX2 9336C-FX2-T y el panel de paso en un gabinete NetApp . Los soportes estándar se incluyen con el interruptor.

Antes de empezar

Asegúrese de tener lo siguiente:

- Para cada interruptor, debe suministrar los ocho tornillos 10-32 o 12-24 y las tuercas de clip para montar los soportes y los rieles deslizantes en los postes delanteros y traseros del gabinete.
- Debe utilizar el kit de riel estándar de Cisco para instalar el switch en un gabinete NetApp .



Los cables puente no están incluidos en el kit de conexión y deben incluirse con los interruptores. Si no se enviaron con los switches, puede pedirlos a NetApp (número de pieza X1558A-R6).

Documentación requerida

Revise los requisitos de preparación inicial, el contenido del kit y las precauciones de seguridad en el ["Guía de instalación de hardware de la serie Cisco Nexus 9000"](#) .

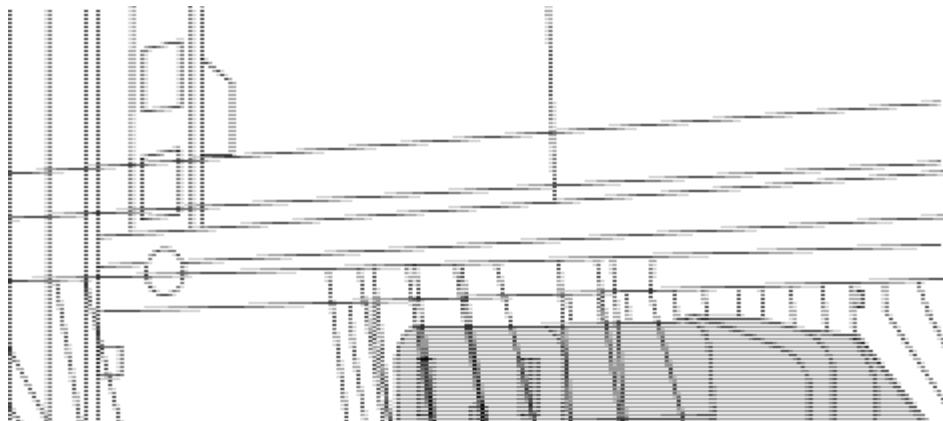
Pasos

1. Instale el panel de obturación de paso en el armario NetApp .

El kit de panel de paso está disponible en NetApp (número de pieza X8784-R6).

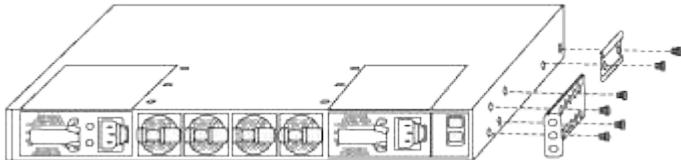
El kit de panel de paso de NetApp contiene el siguiente hardware:

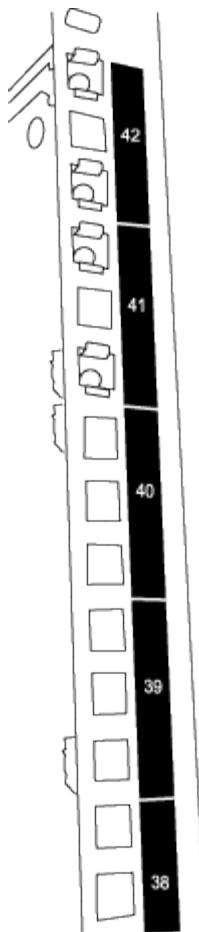
- Un panel ciego pasante
 - Cuatro tornillos 10-32 x .75
 - Cuatro tuercas de clip 10-32
- i. Determine la ubicación vertical de los interruptores y del panel ciego en el gabinete.
En este procedimiento, el panel de obturación se instalará en U40.
 - ii. Instale dos tuercas de clip en cada lado en los orificios cuadrados correspondientes para los rieles del gabinete frontal.
 - iii. Centre el panel verticalmente para evitar la intrusión en el espacio del rack adyacente y luego apriete los tornillos.
 - iv. Inserte los conectores hembra de ambos cables puente de 48 pulgadas desde la parte posterior del panel y a través del conjunto de escobillas.



(1) Conector hembra del cable puente.

2. Instale los soportes de montaje en rack en el chasis del conmutador Nexus 9336C-FX2.
 - a. Coloque un soporte de montaje en rack frontal en un lado del chasis del conmutador de modo que la oreja de montaje esté alineada con la placa frontal del chasis (en el lado de la fuente de alimentación o del ventilador) y luego use cuatro tornillos M4 para fijar el soporte al chasis.
 - b. Repita el paso 2a con el otro soporte de montaje en rack frontal en el otro lado del conmutador.
 - c. Instale el soporte de montaje en rack trasero en el chasis del conmutador.
 - d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del conmutador.
3. Instale las tuercas de clip en las ubicaciones de los orificios cuadrados para los cuatro postes IEA.

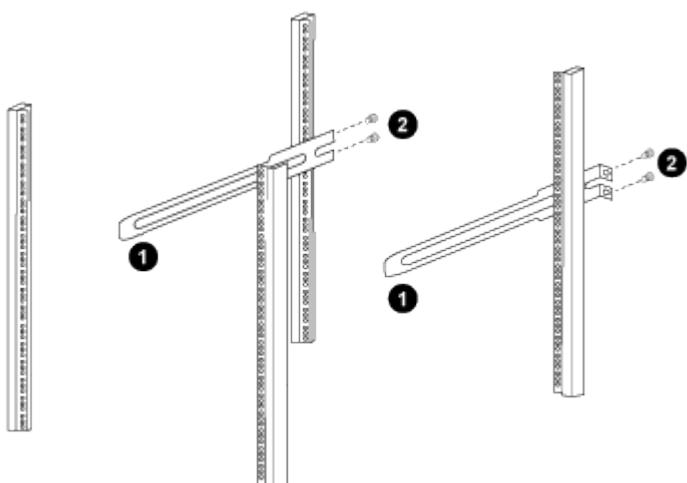




Los dos commutadores 9336C-FX2 siempre se montarán en las 2U superiores del gabinete RU41 y 42.

4. Instale los rieles deslizantes en el gabinete.

- Coloque el primer riel deslizante en la marca RU42 en la parte posterior del poste trasero izquierdo, inserte los tornillos con el tipo de rosca correspondiente y luego apriete los tornillos con los dedos.



(1) Al deslizar suavemente el riel deslizante, alinéelo con los orificios para tornillos del soporte.

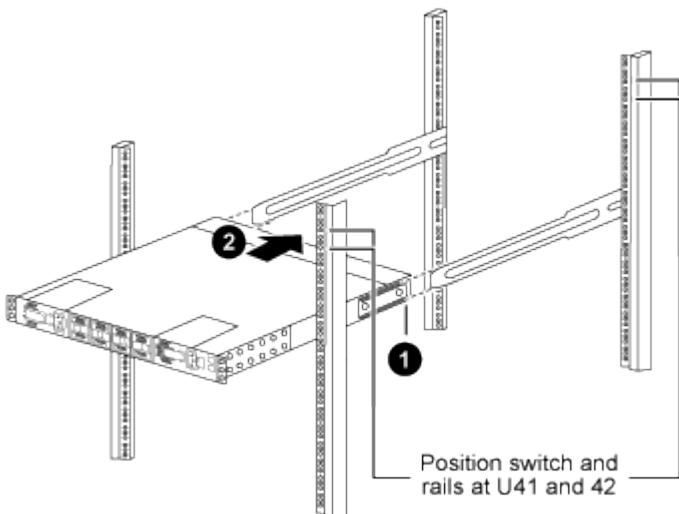
(2) Apriete los tornillos de los rieles deslizantes a los postes del gabinete.

- a. Repita el paso 4a para el poste trasero del lado derecho.
 - b. Repita los pasos 4a y 4b en las ubicaciones RU41 del gabinete.
5. Instale el interruptor en el armario.



Este paso requiere dos personas: una persona para sostener el interruptor desde el frente y otra para guiar el interruptor hacia los rieles deslizantes traseros.

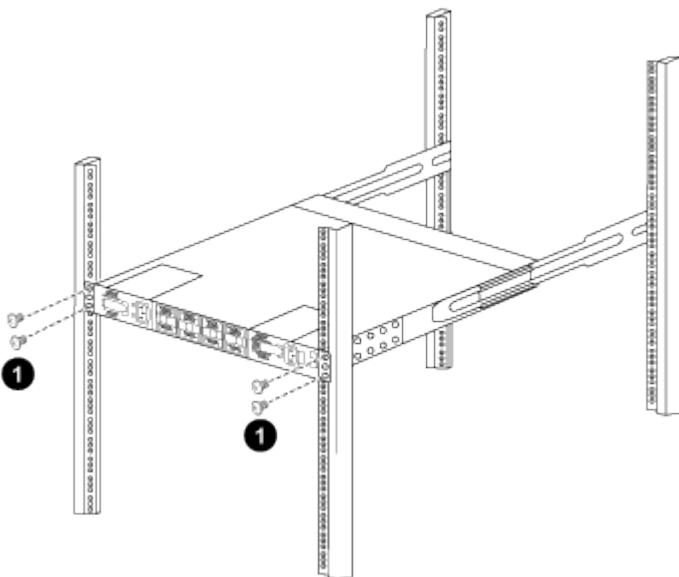
- a. Coloque la parte posterior del interruptor en RU41.



(1) A medida que el chasis se desplaza hacia los postes traseros, alinee las dos guías de montaje del rack trasero con los rieles deslizantes.

(2) Deslice suavemente el interruptor hasta que los soportes de montaje en rack frontales queden al ras con los postes frontales.

- b. Fije el interruptor al armario.



(1) Mientras una persona sujetla la parte frontal del chasis nivelada, la otra persona debe apretar completamente los cuatro tornillos traseros a los postes del gabinete.

- a. Con el chasis ahora apoyado sin ayuda, apriete completamente los tornillos delanteros a los postes.
- b. Repita los pasos 5a a 5c para el segundo interruptor en la ubicación RU42.



Al utilizar el interruptor completamente instalado como soporte, no es necesario sujetar la parte delantera del segundo interruptor durante el proceso de instalación.

6. Cuando los interruptores estén instalados, conecte los cables puente a las entradas de alimentación del interruptor.
7. Conecte los enchufes macho de ambos cables puente a las tomas de corriente PDU más cercanas disponibles.



Para mantener la redundancia, los dos cables deben estar conectados a diferentes PDU.

8. Conecte el puerto de administración de cada comutador 9336C-FX2 a cualquiera de los comutadores de administración (si se solicitaron) o conéctelos directamente a su red de administración.

El puerto de administración es el puerto superior derecho ubicado en el lado de la fuente de alimentación del comutador. El cable CAT6 de cada comutador debe pasarse a través del panel de paso después de instalar los comutadores para conectarlos a los comutadores de administración o a la red de administración.

¿Qué sigue?

Después de instalar los switches en el armario NetApp, puedes ["configurar los comutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T"](#).

Configurar el software

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

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

1

["Configura el interruptor"](#)

Configure los comutadores 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 comutadores 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 comutadores de almacenamiento Cisco 9336C-FX2 y 9336C-FX2-T.

4

"Instalar o actualizar el RCF"

Instale o actualice el RCF después de configurar los comutadores 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 comutadores para usar el Monitor de estado del comutador Ethernet (CSHM) y las funciones de recopilación de registros.

6

"Restablecer el interruptor a los valores predeterminados de fábrica"

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

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

Siga este procedimiento para configurar los comutadores 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 comutadores 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 comutadores 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.

Inmediato	Respuesta
¿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.
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)	<p>Responda con sí. La respuesta predeterminada es sí.</p> <p> 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.</p>

Inmediato	Respuesta
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.
¿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. <div style="display: flex; align-items: center; margin-top: 10px;">  Si no guarda la configuración en este paso, ninguno de los cambios tendrá efecto la próxima vez que reinicie el switch. </div>

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 commutador de interconexión de clúster:

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

Mostrar ejemplo

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

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

-----
-----  

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.

- 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

          Logical          Status      Network
Current      Current  Is
Vserver      Interface
Port        Home
-----  -----
-----  -----
Cluster
        cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01  e0a      true
        cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01  e0b      true
        cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02  e0a      true
        cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02  e0b      true

4 entries were displayed.
```

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

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 `show` comando para mostrar los detalles.

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

		Source	Destination
Packet			
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			

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. 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

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

¿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

          Speed (Mbps)

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

```

b. 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
      Logical          Status      Network
  Current      Current  Is
  Vserver      Interface
  Port        Home
  -----
  -----
Cluster
      cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01  e0a      true
      cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01  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 comutadores 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/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

```
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 Required	Type	EPLD	Running-Version	New-Version	Upg-
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

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

Node: cluster1-02

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

Node: cluster1-03

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

```
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/      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
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                  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
```

```
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:
Unlocking 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 `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date          LIF          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
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

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, reviértala 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 commutadores 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

Nombre RCF
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.

¿Qué 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 commutador. 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 commutador 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. Despues 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 comutadores 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.

¿Qué 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 comutadores (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 comutador asociado operativo mientras se realizan los pasos en el comutador 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 commutadores:

```
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
<hr/>						
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

          Logical          Status      Network      Current
Current Is
Vserver      Interface      Admin/Oper  Address/Mask      Node
Port        Home
-----  -----  -----  -----
-----  -----  -----
Cluster
e7a          node1-01_clus1  up/up      169.254.36.44/16  node1-01
          true
e7b          node1-01_clus2  up/up      169.254.7.5/16   node1-01
          true
          node1-02_clus1  up/up      169.254.197.206/16 node1-02
e7a          true
          node1-02_clus2  up/up      169.254.195.186/16 node1-02
e7b          true
          node1-03_clus1  up/up      169.254.192.49/16  node1-03
e7a          true
          node1-03_clus2  up/up      169.254.182.76/16  node1-03
e7b          true
          node1-04_clus1  up/up      169.254.59.49/16   node1-04
e7a          true
          node1-04_clus2  up/up      169.254.62.244/16  node1-04
e7b          true

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-12-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
AAAAB3NzaC1yc2EAAAQABAAAAgQDiNrD52Q586wTGJjFAbjB1FaA23EpDrZ2sDCew
17nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCD Srp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIBmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
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 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.

Reemplace los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Puede reemplazar los conmutadores Nexus 9336C-FX2 y 9336C-FX2-T defectuosos en una red de clúster. Este es un procedimiento que no produce interrupciones.

Antes de empezar

Antes de instalar el software NX-OS y los RCF en los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T, asegúrese de lo siguiente:

- Su sistema puede admitir los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T.

- Ha consultado la tabla de compatibilidad de switches en la página de switches Ethernet de Cisco para conocer las versiones compatibles de ONTAP, NX-OS y RCF.
- Usted ha consultado el software y las guías de actualización correspondientes disponibles en el sitio web de Cisco .

Switches Cisco Nexus serie 3000:

- Has descargado los formularios RCF correspondientes.
- La configuración de red existente presenta las siguientes características:
 - La página de switches Ethernet de Cisco tiene las últimas versiones de RCF y NX-OS para sus switches.
 - Debe existir conectividad de gestión en ambos comutadores.
- El switch de reemplazo Cisco Nexus 9336C-FX2 tiene las siguientes características:
 - La conectividad de la red de gestión funciona correctamente.
 - El acceso a la consola para el interruptor de repuesto ya está habilitado.
 - La imagen del sistema operativo RCF y NX-OS apropiada se carga en el switch.
 - La configuración inicial del switch está completa.

Acerca de esta tarea

Este procedimiento reemplaza el segundo switch de almacenamiento Nexus 9336C-FX2 S2 con el nuevo switch 9336C-FX NS2. Los dos nodos son nodo1 y nodo2.

Pasos a seguir:

- Confirme que el interruptor que se va a reemplazar es el S2.
- Desconecta los cables del interruptor S2.
- Vuelva a conectar los cables al interruptor NS2.
- Verifique todas las configuraciones de los dispositivos en el switch NS2.



Pueden existir dependencias entre la sintaxis de los comandos en las versiones RCF y NX-OS.

Pasos

1. Si AutoSupport está habilitado en este clúster, suprime la creación automática de casos invocando un mensaje de AutoSupport :

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

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

2. Compruebe el estado de salud de los puertos del nodo de almacenamiento para asegurarse de que existe conexión con el comutador de almacenamiento S1:

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

Mostrar ejemplo

```
storage::*> storage port show -port-type ENET
                                         Speed
                                         (Gb/s)
Node      Port Type  Mode      State    Status   VLAN
-----  -----  -----  -----  -----  -----  -----
node1
        e3a  ENET  storage  100  enabled  online   30
        e3b  ENET  storage   0  enabled  offline   30
        e7a  ENET  storage   0  enabled  offline   30
        e7b  ENET  storage   0  enabled  offline   30
node2
        e3a  ENET  storage  100  enabled  online   30
        e3b  ENET  storage   0  enabled  offline   30
        e7a  ENET  storage   0  enabled  offline   30
        e7b  ENET  storage   0  enabled  offline   30
storage::*>
```

3. Verifique que el conmutador de almacenamiento S1 esté disponible:

```
network device-discovery show
```

Mostrar ejemplo

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol   Port  Device (LLDP: ChassisID)  Interface  Platform
-----  -----  -----
node1/cdp
    e3a    S1
    e4a    node2
    e4e    node2
node1/lldp
    e3a    S1
    e4a    node2
    e4e    node2
node2/cdp
    e3a    S1
    e4a    node1
    e4e    node1
node2/lldp
    e3a    S1
    e4a    node1
    e4e    node1
storage::*>
```

4. Dirigir las cosas `lldp neighbors` Comando en el interruptor de funcionamiento para confirmar que puede ver ambos nodos y todos los estantes:

```
show lldp neighbors
```

Mostrar ejemplo

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf  Hold-time  Capability  Port ID
node1          Eth1/1    121        S           e3a
node2          Eth1/2    121        S           e3a
SHFGD2008000011  Eth1/5    121        S           e0a
SHFGD2008000011  Eth1/6    120        S           e0a
SHFGD2008000022  Eth1/7    120        S           e0a
SHFGD2008000022  Eth1/8    120        S           e0a
```

5. Verifique los puertos de los estantes en el sistema de almacenamiento:

```
storage shelf port show -fields remote-device,remote-port
```

Mostrar ejemplo

```
storage::*> storage shelf port show -fields remote-device,remote-
port
shelf    id    remote-port    remote-device
-----  --  -----
3.20     0    Ethernet1/5    S1
3.20     1    -              -
3.20     2    Ethernet1/6    S1
3.20     3    -              -
3.30     0    Ethernet1/7    S1
3.20     1    -              -
3.30     2    Ethernet1/8    S1
3.20     3    -              -
storage::*>
```

6. Retire todos los cables conectados al interruptor de almacenamiento S2.

7. Vuelva a conectar todos los cables al interruptor de repuesto NS2.

8. Vuelva a comprobar el estado de salud de los puertos del nodo de almacenamiento:

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

Mostrar ejemplo

```
storage::*> storage port show -port-type ENET
                                         Speed
                                         (Gb/s)
Node      Port  Type  Mode      State    Status    VLAN
-----  -----  -----  -----  -----  -----
node1
                    e3a  ENET  storage  100    enabled  online   30
                    e3b  ENET  storage   0    enabled  offline  30
                    e7a  ENET  storage   0    enabled  offline  30
                    e7b  ENET  storage   0    enabled  offline  30
node2
                    e3a  ENET  storage  100    enabled  online   30
                    e3b  ENET  storage   0    enabled  offline  30
                    e7a  ENET  storage   0    enabled  offline  30
                    e7b  ENET  storage   0    enabled  offline  30
storage::*>
```

9. Verifique que ambos interruptores estén disponibles:

```
network device-discovery show
```

Mostrar ejemplo

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----  -----  -----  -----
node1/cdp
    e3a  S1                      Ethernet1/1  NX9336C
    e4a  node2                   e4a          AFF-A700
    e4e  node2                   e4e          AFF-A700
    e7b  NS2                     Ethernet1/1  NX9336C
node1/lldp
    e3a  S1                      Ethernet1/1  -
    e4a  node2                   e4a          -
    e4e  node2                   e4e          -
    e7b  NS2                     Ethernet1/1  -
node2/cdp
    e3a  S1                      Ethernet1/2  NX9336C
    e4a  node1                   e4a          AFF-A700
    e4e  node1                   e4e          AFF-A700
    e7b  NS2                     Ethernet1/2  NX9336C
node2/lldp
    e3a  S1                      Ethernet1/2  -
    e4a  node1                   e4a          -
    e4e  node1                   e4e          -
    e7b  NS2                     Ethernet1/2  -
storage::*>
```

10. Verifique los puertos de los estantes en el sistema de almacenamiento:

```
storage shelf port show -fields remote-device,remote-port
```

Mostrar ejemplo

```
storage::*> storage shelf port show -fields remote-device,remote-
port
shelf    id    remote-port    remote-device
-----  --  -----
3.20     0    Ethernet1/5    S1
3.20     1    Ethernet1/5    NS2
3.20     2    Ethernet1/6    S1
3.20     3    Ethernet1/6    NS2
3.30     0    Ethernet1/7    S1
3.20     1    Ethernet1/7    NS2
3.30     2    Ethernet1/8    S1
3.20     3    Ethernet1/8    NS2
storage::*>
```

11. Si desactivaste la creación automática de casos, vuelve a activarla mediante un mensaje de AutoSupport :

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

¿Que sigue?

Después de haber reemplazado los interruptores, puedes ["configurar la monitorización del estado del conmutador"](#).

Cisco Nexus 3232C

Empezar

Flujo de trabajo de instalación y configuración para los switches de almacenamiento Cisco Nexus 3232C

Los switches Cisco Nexus 3232C forman parte de la plataforma Cisco Nexus 9000 y pueden instalarse en un gabinete de sistema NetApp.

Sigue estos pasos de flujo de trabajo para instalar y configurar tus switches Cisco 3232C.

1

["Revisar los requisitos de configuración"](#)

Revisa los requisitos de configuración de los conmutadores de almacenamiento 3232C.

2

["Revisar la documentación requerida"](#)

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores 3232C y el clúster ONTAP .

3

"Revisar los requisitos de Smart Call Home"

Revise los requisitos de la función Cisco Smart Call Home, que se utiliza para monitorear los componentes de hardware y software de su red.

4

"Instala el hardware"

Instale el hardware del interruptor.

5

"Configurar el software"

Configurar el software del comutador.

Requisitos de configuración para los switches de almacenamiento Cisco Nexus 3232C

Para la instalación y el mantenimiento del switch Cisco Nexus 3232C, asegúrese de revisar los requisitos de configuración y de red.

Requisitos de configuración

Necesitas la cantidad y el tipo adecuados de cables y conectores de cable para tus switches. Dependiendo del tipo de switch que estés configurando al principio, necesitas conectarte al puerto de consola del switch con el cable de consola incluido; también necesitas proporcionar información de red específica.

Requisitos de red

Necesitará la siguiente información de red para todas las configuraciones de comutadores:

- Subred IP para la gestión del tráfico de red
- Nombres de host y direcciones IP para cada uno de los controladores del sistema de almacenamiento y todos los comutadores aplicables
- La mayoría de los controladores del sistema de almacenamiento se administran a través de la interfaz e0M conectándose al puerto de servicio Ethernet (ícono de llave inglesa). En los sistemas AFF A800 y AFF A700, la interfaz e0M utiliza un puerto Ethernet dedicado.

Consulte el "[Hardware Universe](#)" Para obtener la información más reciente. Ver "[¿Qué información adicional necesito para instalar mi equipo que no está en HWU?](#)" para obtener más información sobre los requisitos de instalación del comutador.

¿Qué sigue?

Después de que hayas confirmado tus requisitos de configuración, puedes revisar la "[documentación requerida](#)".

Requisitos de documentación para los switches de almacenamiento Cisco Nexus 3232C

Para la instalación y el mantenimiento del switch Cisco Nexus 3232C, asegúrese de revisar toda la documentación recomendada.

Documentación del interruptor

Para configurar los switches Cisco Nexus 3232C, necesita la siguiente documentación de ["Soporte para switches Cisco Nexus serie 3000"](#) página.

Título del documento	Descripción
<i>Guía de instalación de hardware de la serie Nexus 3000</i>	Proporciona información detallada sobre los requisitos del sitio, detalles del hardware del switch y opciones de instalación.
<i>Guías de configuración de software para switches Cisco Nexus serie 3000 (elija la guía correspondiente a la versión de NX-OS instalada en sus switches)</i>	Proporciona la información de configuración inicial del switch que necesita antes de poder configurarlo para el funcionamiento de ONTAP .
<i>Guía de actualización y degradación de software NX-OS de la serie Cisco Nexus 3000 (elija la guía correspondiente a la versión de NX-OS instalada en sus switches)</i>	Proporciona información sobre cómo degradar el software del switch a uno compatible con ONTAP , si fuera necesario.
<i>Índice maestro de referencia de comandos de Cisco Nexus serie 3000 NX-OS</i>	Proporciona enlaces a las diversas referencias de comandos proporcionadas por Cisco.
<i>Referencia de MIB de Cisco Nexus 3000</i>	Describe los archivos de la Base de Información de Gestión (MIB) para los switches Nexus 3000.
<i>Referencia de mensajes del sistema NX-OS de la serie Nexus 3000</i>	Describe los mensajes del sistema para los switches Cisco Nexus serie 3000, aquellos que son informativos y otros que podrían ayudar a diagnosticar problemas con los enlaces, el hardware interno o el software del sistema.
<i>Notas de la versión de NX-OS de la serie Cisco Nexus 3000 (elija las notas correspondientes a la versión de NX-OS instalada en sus switches)</i>	Describe las características, errores y limitaciones de la serie Cisco Nexus 3000.
Información normativa, de cumplimiento y de seguridad para las series Cisco Nexus 6000, Cisco Nexus 5000, Cisco Nexus 3000 y Cisco Nexus 2000.	Proporciona información sobre cumplimiento normativo, seguridad y requisitos legales de organismos internacionales para los switches de la serie Nexus 3000.

Documentación de los sistemas ONTAP

Para configurar un sistema ONTAP , necesita los siguientes documentos para su versión del sistema operativo de ["ONTAP 9"](#) .

Nombre	Descripción
Instrucciones de instalación y configuración específicas del controlador	Describe cómo instalar el hardware de NetApp .
Documentación de ONTAP	Proporciona información detallada sobre todos los aspectos de las versiones de ONTAP .
"Hardware Universe"	Proporciona información sobre la configuración y compatibilidad del hardware de NetApp .

Documentación del kit de rieles y del gabinete

Para instalar un switch Cisco 3232C en un gabinete NetApp , consulte la siguiente documentación de hardware.

Nombre	Descripción
"Gabinete de sistema 42U, guía profunda"	Describe las FRU asociadas con el gabinete del sistema 42U y proporciona instrucciones de mantenimiento y reemplazo de FRU.
"Instale un switch Cisco Nexus 3232C en un gabinete NetApp"	Describe cómo instalar un switch Cisco Nexus 3232C en un gabinete NetApp de cuatro postes.

Requisitos de Smart Call Home

Para utilizar Smart Call Home, debe configurar un conmutador de red de clúster para comunicarse mediante correo electrónico con el sistema Smart Call Home. Además, puede configurar opcionalmente su conmutador de red de clúster para aprovechar la función de soporte Smart Call Home integrada de Cisco.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Antes de poder utilizar Smart Call Home, tenga en cuenta los siguientes requisitos:

- Debe haber un servidor de correo electrónico instalado.
- El switch debe tener conectividad IP con el servidor de correo electrónico.
- Debe configurarse el nombre del contacto (contacto del servidor SNMP), el número de teléfono y la información de la dirección postal. Esto es necesario para determinar el origen de los mensajes recibidos.
- Debe asociarse un ID de CCO con un contrato de servicio Cisco SMARTnet apropiado para su empresa.
- El servicio Cisco SMARTnet debe estar instalado para que el dispositivo pueda registrarse.

Instalar hardware

Flujo de trabajo de instalación de hardware para comutadores Cisco Nexus 3232C

Para instalar y configurar el hardware de un comutador de almacenamiento 3232C, sigue estos pasos:

1

"Instala el interruptor"

Instala el comutador de almacenamiento 3232C.

2

"Instale el switch en un armario NetApp"

Instala el comutador de almacenamiento 3232C y el panel de paso en un armario NetApp según sea necesario.

Instala el comutador de almacenamiento 3232C

Sigue este procedimiento para instalar y configurar el comutador de almacenamiento Cisco Nexus 3232C.

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 del archivo de configuración de referencia (RCF).
- Versión aplicable de NX-OS, descargada de ["Descarga de software de Cisco"](#) página.
- Licencias aplicables, información de red y configuración, y cables.
- 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 comutadores también tienen la versión actual del software NX-OS pero no tienen los RCF cargados.
- ["Documentación necesaria del switch y del ONTAP"](#).

Pasos

1. Instale en rack los comutadores y controladores de la red del clúster y de la red de administración.

Si estás instalando...	Entonces...
Cisco Nexus 3232C en un gabinete de sistema NetApp	Consulte la guía <u>Instalación de un comutador de clúster Cisco Nexus 3232C y un panel de paso en un gabinete NetApp</u> para obtener instrucciones sobre cómo instalar el comutador en un gabinete NetApp .

Si estás instalando...	Entonces...
Equipos en un rack de telecomunicaciones	Consulte los procedimientos proporcionados en las guías de instalación del hardware del switch y las instrucciones de instalación y configuración de NetApp .

2. Conecte los conmutadores de red del clúster y de la red de administración a los controladores utilizando las hojas de trabajo de cableado completadas.
3. Encienda la alimentación de los conmutadores y controladores de la red del clúster y de la red de administración.

¿Que sigue?

Después de que hayas instalado el conmutador de almacenamiento 3232C, puedes ["Instala el conmutador en un armario NetApp"](#).

Instala un switch de almacenamiento Cisco Nexus 3232C en un armario NetApp

Dependiendo de tu configuración, puede que necesites instalar el switch de almacenamiento Cisco Nexus 3232C y el panel de paso en un gabinete de NetApp con los soportes estándar que vienen incluidos con el switch.

Antes de empezar

Verifica que tienes lo siguiente: * Los requisitos de preparación inicial, el contenido del kit y las precauciones de seguridad en el ["Guía de instalación de hardware de la serie Cisco Nexus 3000"](#). * Para cada switch, los ocho tornillos 10-32 o 12-24 y las tuercas de clip para montar los soportes y los raíles deslizantes en los postes delantero y trasero del armario. * Kit de raíles estándar de Cisco para instalar el switch en un armario NetApp.



Los cables puente no están incluidos en el kit de conexión y deben incluirse con los interruptores. Si no se enviaron con los switches, puede pedirlos a NetApp (número de pieza X1558A-R6).

Pasos

1. Instale el panel de obturación de paso en el armario NetApp .

El kit de panel de paso está disponible en NetApp (número de pieza X8784-R6).

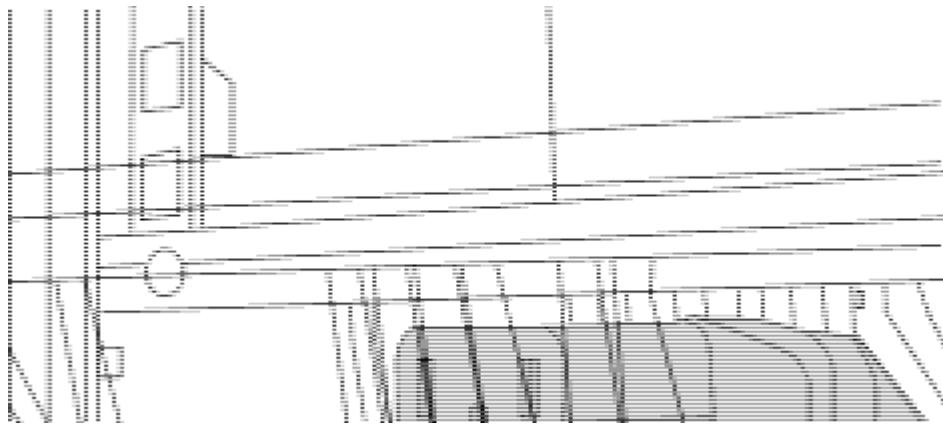
El kit de panel de paso de NetApp contiene el siguiente hardware:

- Un panel ciego pasante
 - Cuatro tornillos 10-32 x .75
 - Cuatro tuercas de clip 10-32
- i. Determine la ubicación vertical de los interruptores y del panel ciego en el gabinete.

En este procedimiento, el panel de obturación se instalará en U40.

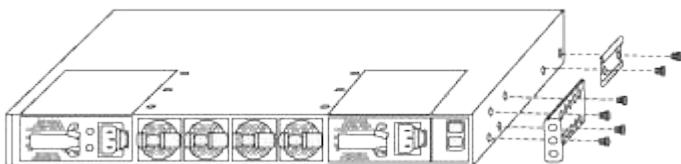
- ii. Instale dos tuercas de clip en cada lado en los orificios cuadrados correspondientes para los rieles del gabinete frontal.
- iii. Centre el panel verticalmente para evitar la intrusión en el espacio del rack adyacente y luego apriete los tornillos.

- iv. Inserte los conectores hembra de ambos cables puente de 48 pulgadas desde la parte posterior del panel y a través del conjunto de escobillas.

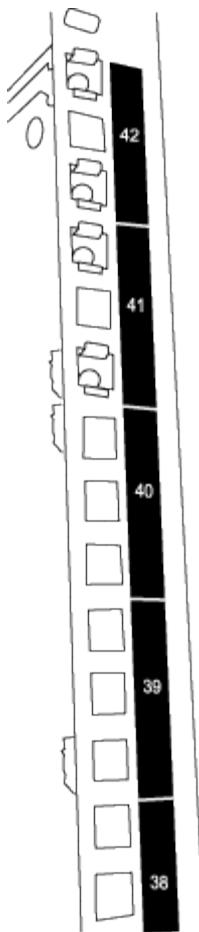


(1) Conector hembra del cable puente.

1. Instala los soportes de montaje en bastidor en el chasis del comutador de almacenamiento Nexus 3232C.
 - a. Coloque un soporte de montaje en rack frontal en un lado del chasis del comutador de modo que la oreja de montaje esté alineada con la placa frontal del chasis (en el lado de la fuente de alimentación o del ventilador) y luego use cuatro tornillos M4 para fijar el soporte al chasis.



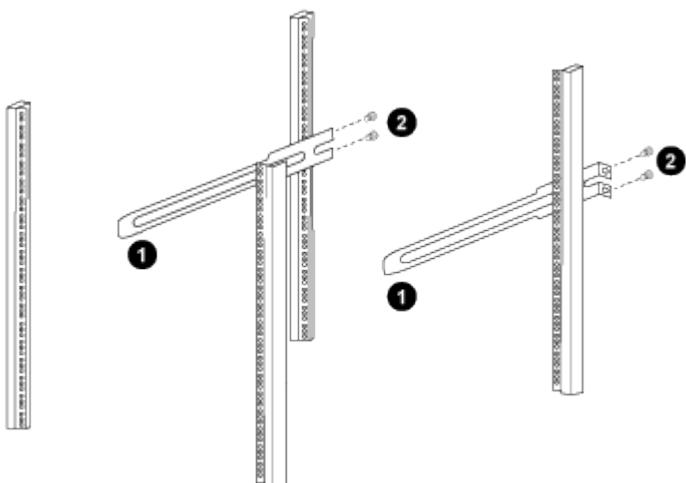
- b. Repita el paso 2a con el otro soporte de montaje en rack frontal en el otro lado del comutador.
 - c. Instale el soporte de montaje en rack trasero en el chasis del comutador.
 - d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del comutador.
2. Instale las tuercas de clip en las ubicaciones de los orificios cuadrados para los cuatro postes IEA.



Los dos interruptores 3232C siempre se montarán en las 2U superiores del gabinete RU41 y 42.

3. Instale los rieles deslizantes en el gabinete.

- a. Coloque el primer riel deslizante en la marca RU42 en la parte posterior del poste trasero izquierdo, inserte los tornillos con el tipo de rosca correspondiente y luego apriete los tornillos con los dedos.



(1) Al deslizar suavemente el riel deslizante, alinéelo con los orificios para tornillos del estante. + (2) Apriete los tornillos de los rieles deslizantes a los postes del gabinete.

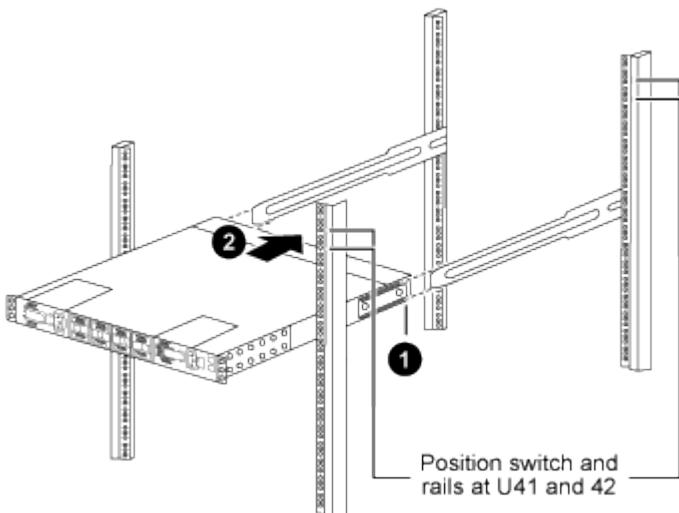
- a. Repita el paso 4a para el poste trasero del lado derecho.

- b. Repita los pasos 4a y 4b en las ubicaciones RU41 del gabinete.
4. Instale el interruptor en el armario.



Este paso requiere dos personas: una persona para sostener el interruptor desde el frente y otra para guiar el interruptor hacia los rieles deslizantes traseros.

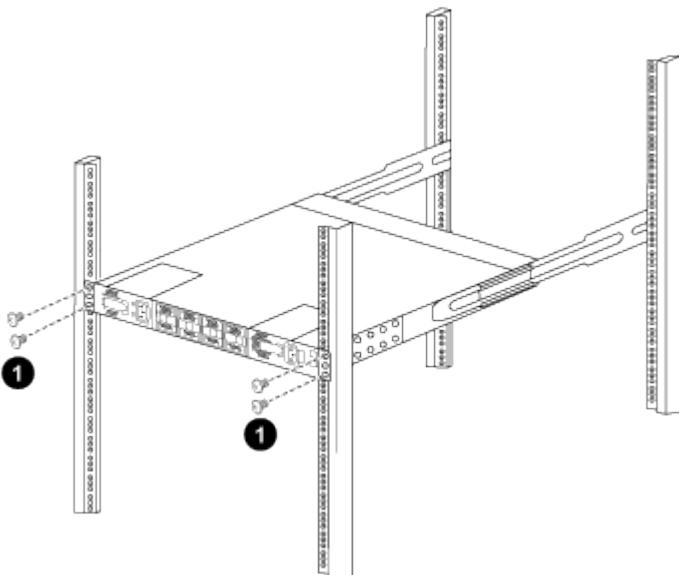
- a. Coloque la parte posterior del interruptor en RU41.



(1) A medida que el chasis se desplaza hacia los postes traseros, alinee las dos guías de montaje del rack trasero con los rieles deslizantes.

(2) Deslice suavemente el interruptor hasta que los soportes de montaje en rack frontales queden al ras con los postes frontales.

- b. Fije el interruptor al armario.



(1) Mientras una persona sujetla la parte frontal del chasis nivelada, la otra persona debe apretar completamente los cuatro tornillos traseros a los postes del gabinete.

- a. Con el chasis ahora apoyado sin ayuda, apriete completamente los tornillos delanteros a los postes.

b. Repita los pasos 5a a 5c para el segundo interruptor en la ubicación RU42.



Al utilizar el interruptor completamente instalado como soporte, no es necesario sujetar la parte delantera del segundo interruptor durante el proceso de instalación.

5. Cuando los interruptores estén instalados, conecte los cables puente a las entradas de alimentación del interruptor.
6. Conecte los enchufes macho de ambos cables puente a las tomas de corriente PDU más cercanas disponibles.



Para mantener la redundancia, los dos cables deben estar conectados a diferentes PDU.

7. Conecte el puerto de administración de cada commutador 3232C a cualquiera de los commutadores de administración (si se solicitaron) o conéctelos directamente a su red de administración.

El puerto de administración es el puerto superior derecho ubicado en el lado de la fuente de alimentación del commutador. El cable CAT6 de cada commutador debe pasarse a través del panel de paso después de instalar los commutadores para conectarlos a los commutadores de administración o a la red de administración.

Configurar software

Flujo de trabajo de instalación de software para switches de almacenamiento Cisco Nexus 3232C

Para instalar y configurar el software de un commutador Cisco Nexus 3232C e instalar o actualizar el archivo de configuración de referencia (RCF), siga estos pasos:

1

"Configura el interruptor"

Configura el commutador de almacenamiento 3232C.

2

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

El software Cisco NX-OS y los archivos de configuración de referencia (RCFs) deben instalarse en los commutadores de almacenamiento Cisco 3232C.

3

"Instale el software NX-OS"

Descarga e instala o actualiza el software NX-OS en el commutador de almacenamiento Cisco 3232C.

4

"Instala el RCF"

Instala el RCF después de configurar el commutador de almacenamiento Cisco 3232C por primera vez.

5

"Verificar la configuración SSH"

Verifique que SSH esté habilitado en los commutadores para usar el Monitor de estado del commutador

Ethernet (CSHM) y las funciones de recopilación de registros.

6

"Restablecer el interruptor a los valores predeterminados de fábrica"

Borra la configuración del switch de almacenamiento 3232C.

Configura el conmutador de almacenamiento 3232C

Siga este procedimiento para instalar y configurar el conmutador Cisco Nexus 3232C.

Antes de empezar

- 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.
- Documentación requerida para la red del clúster y el conmutador de red de administración.

Consulta "["Documentación requerida"](#) para más información.

- Documentación requerida del controlador y documentación de ONTAP .

"Documentación de NetApp"

- Licencias aplicables, información de red y configuración, y cables.
- Hojas de trabajo de cableado completadas.
- Los archivos RCF de red de clúster y de red de administración de NetApp aplicables se pueden descargar del sitio de soporte de NetApp en "["mysupport.netapp.com"](#) para los interruptores que reciba. 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 cargados los RCF.

Pasos

1. Instale en rack los conmutadores y controladores de la red del clúster y de la red de administración.

Si estás instalando tu...	Entonces...
Cisco Nexus 3232C en un gabinete de sistema NetApp	Consulta la guía <i>Installing a Cisco Nexus 3232C switch and pass-through panel in a NetApp cabinet</i> para ver las instrucciones para instalar el switch en un armario NetApp.
Equipos en un rack de telecomunicaciones	Consulte los procedimientos proporcionados en las guías de instalación del hardware del switch y las instrucciones de instalación y configuración de NetApp .

2. Conecte los conmutadores de red del clúster y de la red de administración a los controladores utilizando las hojas de trabajo de cableado completadas.
3. Encienda la alimentación de los conmutadores y controladores de la red del clúster y de la red de administración.
4. 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.
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.

Inmediato	Respuesta
¿Servicio SSH habilitado? (sí/no)	<p>Responda con sí. La respuesta predeterminada es sí.</p> <p> 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.</p>
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 entre 1024 y 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.
¿Desea editar la configuración? (sí/no)	<p>En este punto debería ver la nueva configuración. Revise y realice los cambios necesarios en la configuración que acaba de ingresar.</p> <p>Responda con no cuando se le solicite si está satisfecho con la configuración. Responda con sí si desea editar su configuración.</p>
¿Usar esta configuración y guardarla? (sí/no)	<p>Responda con sí para guardar la configuración. Esto actualiza automáticamente las imágenes de kickstart y del sistema.</p> <p> Si no guarda la configuración en este paso, ninguno de los cambios tendrá efecto la próxima vez que reinicie el switch.</p>

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

¿Que sigue?

Después de que hayas configurado tus switches, puedes ["Prepárese para instalar NX-OS y RCF."](#).

Preparar la instalación del software NX-OS y el archivo de configuración de referencia (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 dos nodos. Estos nodos utilizan dos puertos de interconexión de clúster 10GbE. e0a y e0b.

Ver el ["Hardware Universe"](#) para verificar los puertos de clúster correctos en sus plataformas. Ver ["¿Qué información adicional necesito para instalar mi equipo que no está en HWU?"](#) para obtener más información sobre los requisitos de instalación del conmutador.



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

Nomenclatura de interruptores y nodos

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 de los clústeres LIF son cluster1-01_clus1 y cluster1-01_clus2 para el clúster 1-01 y cluster1-02_clus1 y cluster1-02_clus2 para el clúster 1-02.
- 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 3000; se utilizan comandos ONTAP a menos que se indique lo contrario.

Pasos

1. Si AutoSupport está habilitado en este clúster, suprime 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 suprime 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 cdp
```

Mostrar ejemplo

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

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

-----
-----  

cluster1-02/cdp
      e0a    cs1          Eth1/2      N3K-
C3232C
      e0b    cs2          Eth1/2      N3K-
C3232C
cluster1-01/cdp
      e0a    cs1          Eth1/1      N3K-
C3232C
      e0b    cs2          Eth1/1      N3K-
C3232C

4 entries were displayed.
```

4. 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
      Speed (Mbps)  Health
Port    IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
-----  -----
e0a     Cluster      Cluster          up    9000  auto/10000
      healthy
e0b     Cluster      Cluster          up    9000  auto/10000
      healthy

Node: cluster1-01
      Speed (Mbps)  Health
Port    IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
-----  -----
e0a     Cluster      Cluster          up    9000  auto/10000
      healthy
e0b     Cluster      Cluster          up    9000  auto/10000
      healthy

4 entries were displayed.
```

a. Mostrar información sobre los LIF:

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

Mostrar ejemplo

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

          Logical          Status      Network
Current      Current  Is
Vserver      Interface
Port        Home
-----  -----
-----  -----
Cluster
        cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01  e0a      true
        cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01  e0b      true
        cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02  e0a      true
        cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02  e0b      true

4 entries were displayed.
```

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

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 `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date          LIF          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 6]] Verifique que el auto-revert El comando está habilitado en todos los LIF del clúster:
`network interface show -vserver Cluster -fields auto-revert`

Mostrar ejemplo

```

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

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

```

¿Que sigue?

Después de que te hayas preparado para instalar el software NX-OS y RCF, puedes ["Instalar el software NX-OS"](#).

Instale el software NX-OS

Puedes usar este procedimiento para instalar el software NX-OS en el comutador de almacenamiento Nexus 3232C.

Requisitos de revisión

Antes de empezar

Verifica que tienes lo siguiente: * Una copia de seguridad actual de la configuración del switch. * Un clúster en pleno funcionamiento (sin errores en los registros ni problemas similares). * ["página del switch Ethernet de Cisco"](#). Consulta la tabla de compatibilidad de switches para las versiones compatibles de ONTAP y NX-OS. * ["Switches Cisco Nexus serie 3000"](#). Consulta las guías de software y actualización adecuadas disponibles en el sitio web de Cisco para la documentación completa sobre los procedimientos de actualización y downgrade de switches Cisco.

Instala el software

El procedimiento requiere el uso de comandos ONTAP y comandos de switches Cisco Nexus serie 3000; se utilizan comandos ONTAP a menos que se indique lo contrario.

Completa el procedimiento en ["Prepárese para instalar NX-OS y RCF."](#) y luego sigue los pasos a continuación.

Pasos

1. Conecte el comutador del clúster a la red de administración.
2. Utilice el `ping` comando 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
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 comutadores 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
C3232C
    e0d    cs2
C3232C
cluster1-02/cdp
    e0a    cs1
C3232C
    e0d    cs2
C3232C
cluster1-03/cdp
    e0a    cs1
C3232C
    e0b    cs2
C3232C
cluster1-04/cdp
    e0a    cs1
C3232C
    e0b    cs2
C3232C
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 -role cluster
```

Mostrar ejemplo

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```

Node: cluster1-04

Ignore

          Speed (Mbps)

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

```

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

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

Mostrar ejemplo

```
cluster1::*> network interface show -role cluster
      Logical          Status      Network
  Current      Current  Is
  Vserver      Interface
  Port        Home
  -----
  -----
  Cluster
      cluster1-01_clus1  up/up      169.254.3.4/23
  cluster1-01  e0a      true
      cluster1-01_clus2  up/up      169.254.3.5/23
  cluster1-01  e0d      true
      cluster1-02_clus1  up/up      169.254.3.8/23
  cluster1-02  e0a      true
      cluster1-02_clus2  up/up      169.254.3.9/23
  cluster1-02  e0d      true
      cluster1-03_clus1  up/up      169.254.1.3/23
  cluster1-03  e0a      true
      cluster1-03_clus2  up/up      169.254.1.1/23
  cluster1-03  e0b      true
      cluster1-04_clus1  up/up      169.254.1.6/23
  cluster1-04  e0a      true
      cluster1-04_clus2  up/up      169.254.1.7/23
  cluster1-04  e0b      true
  8 entries were displayed.
cluster1::*>
```

- c. Verifique que el clúster muestre información para ambos comutadores 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      N3K-
C3232C
    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      N3K-
C3232C
    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 3232C.

Mostrar ejemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.4.bin /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

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

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) 2002-2019, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own

licenses, such as open source. This software is provided "as is,"
and unless

otherwise stated, there is no warranty, express or implied,
including but not

limited to warranties of merchantability and fitness for a
particular purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/library.txt.
```

Software

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

Hardware

```
cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
```

```
Processor Board ID FOCXXXXXXGD
```

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

```
Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(3)
Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

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

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

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

Compatibility check is done:
Module  bootable          Impact          Install-type  Reason
-----  -----
-----  -----
1      Yes            Disruptive      Reset          Default
upgrade is not hitless

Images will be upgraded according to following table:
Module      Image      Running-Version(pri:alt)
New-Version  Upg-Required
-----  -----
-----  -----
1          nxos      9.3(3)
9.3(4)          yes
1          bios      v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(01/28/2020)  no

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

```
Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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

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

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/library.txt.
```

Software

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

Hardware

```
cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
```

```
Processor Board ID FOCXXXXXXGS
```

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

```
Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
Reason: Reset due to upgrade
```

```
System version: 9.3(3)
Service:

plugin
Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

10. Actualice la imagen EPLD y reinicie el switch.

Mostrar ejemplo

```
cs2# show version module 1 epld

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

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

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

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

11. Si va a actualizar a la versión 9.3(11) de NX-OS, debe actualizar el EPLD. golden Imagen y reinicie el switch una vez más. De lo contrario, pase al paso 12.

Ver "Notas de la versión de actualización de EPLD, versión 9.3(11)" Para obtener más detalles.

Mostrar ejemplo

```
cs2# install epld bootflash:n9000-epld.9.3.11.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module          Type          Upgradable      Impact      Reason
-----          -----          -----          Disruptive  Module
-----          -----          -----          Upgradable

1             SUP           Yes

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

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

12. Tras reiniciar el switch, inicie sesión para verificar que la nueva versión de EPLD se haya cargado correctamente.

Mostrar ejemplo

```
cs2# show version module 1 epld

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

13. 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 -role cluster
```

Mostrar ejemplo

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0d	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
8 entries were displayed.
```

b. Verifique el estado del switch desde el clúster.

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

Mostrar ejemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----
cluster1-01/cdp
      e0a    cs1          Ethernet1/7      N3K-
C3232C
      e0d    cs2          Ethernet1/7      N3K-
C3232C
cluster01-2/cdp
      e0a    cs1          Ethernet1/8      N3K-
C3232C
      e0d    cs2          Ethernet1/8      N3K-
C3232C
cluster01-3/cdp
      e0a    cs1          Ethernet1/1/1    N3K-
C3232C
      e0b    cs2          Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
      e0a    cs1          Ethernet1/1/2    N3K-
C3232C
      e0b    cs2          Ethernet1/1/2    N3K-
C3232C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch          Type          Address
Model

-----
-----
cs1            cluster-network  10.233.205.90  N3K-
C3232C
  Serial Number: 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  N3K-
```

```
C3232C
```

```
    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:
Unlocking 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.
```

14. 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::*
```

15. Repita los pasos 6 a 14 en el interruptor cs1.

16. Habilitar la reversión automática en los LIF del clúster.

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

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

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

Mostrar ejemplo

```
cluster1::*> network interface show -role cluster
      Logical          Status      Network      Current
Current Is
Vserver      Interface      Admin/Oper  Address/Mask      Node
Port        Home
-----
-----
Cluster
      cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01      e0d      true
      cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01      e0d      true
      cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02      e0d      true
      cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02      e0d      true
      cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03      e0b      true
      cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03      e0b      true
      cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04      e0b      true
      cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04      e0b      true
8 entries were displayed.
cluster1::*
```

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

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

¿Que sigue?

Después de haber instalado el software NX-OS, puedes ["instalar o actualizar el archivo de configuración de referencia \(RCF\)".](#)

Instalar el archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar los conmutadores Nexus 3232C por primera vez.

Antes de empezar

Verifique las siguientes instalaciones y conexiones:

- 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.
- Una conexión de consola al switch, esto es necesario cuando se instala el RCF.

Acerca de esta tarea

El procedimiento requiere el uso de comandos ONTAP y comandos de switches Cisco Nexus serie 3000; se utilizan comandos ONTAP a menos que se indique lo contrario.

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 habilitar operaciones de clúster sin interrupciones, el siguiente procedimiento migra todos los LIF del clúster al conmutador del socio operativo mientras se realizan los pasos en el conmutador de destino.

Completa el procedimiento en ["Prepárese para instalar NX-OS y RCF."](#) y luego sigue los pasos a continuación.

Paso 1: Instale el RCF en los interruptores

1. Inicie sesión para cambiar cs2 usando SSH o mediante una consola serial.
2. Copie el RCF al bootflash del conmutador cs2 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 3000 NX-OS"](#) .

Mostrar ejemplo

Este ejemplo muestra cómo se utiliza TFTP para copiar un RCF a la memoria flash de arranque del switch cs2:

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

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 3000 NX-OS"](#) .

Mostrar ejemplo

Este ejemplo muestra el archivo RCF. `Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt` Instalando en el switch cs2:

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



Asegúrate de leer detenidamente las secciones **Installation notes**, **Important Notes** y **banner** de tu RCF. Debes leer y seguir estas instrucciones para verificar la correcta configuración y funcionamiento del switch.

4. Examine la salida del banner de `show banner motd` dominio. Debe leer y seguir las instrucciones que figuran en **Notas importantes** para garantizar la configuración y el funcionamiento correctos del interruptor.
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. Vuelva a aplicar cualquier personalización anterior a la configuración del switch.
7. 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 administración * Puerta de enlace predeterminada * Nombre del conmutador

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

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

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region qos 256" >>
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.

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

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

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

```
cs2# write erase
```

```
Warning: This command will erase the startup-configuration.
```

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

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

```
cs2# copy bootflash:write_erase.cfg startup-config
```

12. Interruptor de reinicio cs2:

```
cs2# reload
```

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

13. Repita los pasos 1 a 12 en el interruptor cs1.

14. Conecte los puertos del clúster de todos los nodos del clúster ONTAP a los comutadores cs1 y cs2.

Paso 2: Verifique las conexiones del conmutador

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

```
show interface brief | grep up
```

Mostrar ejemplo

```
cs1# show interface brief | grep up
.
.
.
Eth1/1/1      1      eth  access  up      none
10G(D)  --
Eth1/1/2      1      eth  access  up      none
10G(D)  --
Eth1/7      1      eth  trunk   up      none
100G(D)  --
Eth1/8      1      eth  trunk   up      none
100G(D)  --
.
.
```

2. Verifique que el ISL entre cs1 y cs2 sea funcional:

```
show port-channel summary
```

Mostrar 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      Eth1/31 (P)  Eth1/32 (P)
cs1#
```

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

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

Mostrar ejemplo

```
cluster1::*> network interface show -role cluster
      Logical          Status      Network      Current
Current Is
Vserver      Interface      Admin/Oper  Address/Mask      Node
Port        Home
-----
-----
Cluster
      cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01      e0d      true
      cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01      e0d      true
      cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02      e0d      true
      cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02      e0d      true
      cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03      e0b      true
      cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03      e0b      true
      cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04      e0b      true
      cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04      e0b      true
8 entries were displayed.
cluster1::*>
```

Si algún LIFS del clúster no ha regresado a sus puertos de origen, reviértalo manualmente:

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

4. 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::*>
```

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 y el establecimiento de un clúster, incluida la asignación de una dirección IP de administración de nodo, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento de almacenamiento inicial.

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

¿Que sigue?

Una vez instalado 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
AAAAB3NzaC1yc2EAAAQABAAAAgQDiNrD52Q586wTGJjFAbjB1FaA23EpDrZ2sDCew
17nwlioC6HBejxluI0bAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCD Srp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIBmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
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 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?

Una vez que hayas verificado tu configuración SSH, podrás "["configurar la monitorización del estado del conmutador"](#).

Restablece el conmutador de almacenamiento 3232C a los valores predeterminados de fábrica

Para restablecer los valores predeterminados de fábrica del conmutador de almacenamiento 3232C, tienes que borrar la configuración del conmutador de almacenamiento 3232C.

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 restablecer el interruptor, puedes [“reconfigurar”](#) según tus necesidades.

Reemplazar un switch de almacenamiento Cisco Nexus 3232C

Siga estos pasos para reemplazar un switch de almacenamiento Cisco Nexus 3232C defectuoso. Este es un procedimiento que no produce interrupciones.

Requisitos de revisión

La configuración de red existente debe tener las siguientes características:

- La página de switches Ethernet de Cisco tiene las últimas versiones de RCF y NX-OS para sus switches.
- Debe existir conectividad de gestión en ambos conmutadores.



Asegúrese de que se hayan completado todos los pasos de solución de problemas para confirmar que su interruptor necesita ser reemplazado.

El switch de reemplazo Cisco Nexus 3232C debe tener las siguientes características:

- La conectividad de la red de gestión debe funcionar correctamente.
- Debe estar habilitado el acceso a la consola para el interruptor de repuesto.
- La imagen del sistema operativo RCF y NX-OS apropiada debe cargarse en el switch.
- La personalización inicial del interruptor debe estar completa.

Reemplace el interruptor

Este procedimiento reemplaza el segundo switch de almacenamiento Nexus 3232C S2 con el nuevo switch 3232C NS2. Los dos nodos son nodo1 y nodo2.

Paso 1: Confirme que el interruptor que se va a reemplazar es el S2.

1. Si AutoSupport está habilitado en este clúster, suprime la creación automática de casos invocando un mensaje de AutoSupport :

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

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. Compruebe el estado de salud de los puertos del nodo de almacenamiento para asegurarse de que existe conexión con el conmutador de almacenamiento S1:

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

Mostrar ejemplo

```
storage::*> storage port show -port-type ENET
                                         Speed
                                         (Gb/s)
Node      Port Type  Mode      State   Status   VLAN   ID
-----  -----  -----  -----  -----  -----  -----  -----
node1
          e3a  ENET  storage    100  enabled  online   30
          e3b  ENET  storage     0  enabled  offline  30
          e7a  ENET  storage     0  enabled  offline  30
          e7b  ENET  storage     0  enabled  offline  30
node2
          e3a  ENET  storage    100  enabled  online   30
          e3b  ENET  storage     0  enabled  offline  30
          e7a  ENET  storage     0  enabled  offline  30
          e7b  ENET  storage     0  enabled  offline  30
```

3. Verifique que el conmutador de almacenamiento S1 esté disponible:

```
network device-discovery show
```

Mostrar ejemplo

```
storage::*# network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----
node1/cdp
    e3a    S1
NX3232C
    e4a    node2
A700
    e4e    node2
A700
node1/lldp
    e3a    S1
    e4a    node2
    e4e    node2
node2/cdp
    e3a    S1
NX3232C
    e4a    node1
A700
    e4e    node1
A700
node2/lldp
    e3a    S1
    e4a    node1
    e4e    node1
```

4. Ejecutar el show lldp neighbors Comando en el interruptor de funcionamiento para confirmar que puede ver ambos nodos y todos los estantes:

```
show lldp neighbors
```

Mostrar ejemplo

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID          Local Intf      Hold-time  Capability  Port
ID
node1             Eth1/1        121          S          e3a
node2             Eth1/2        121          S          e3a
SHFGD2008000011  Eth1/5        121          S          e0a
SHFGD2008000011  Eth1/6        120          S          e0a
SHFGD2008000022  Eth1/7        120          S          e0a
SHFGD2008000022  Eth1/8        120          S          e0a
```

Paso 2: Configurar el cableado

1. Verifique los puertos de los estantes en el sistema de almacenamiento:

```
storage shelf port show -fields remote-device,remote-port
```

Mostrar ejemplo

```
storage::*> storage shelf port show -fields remote-device,remote-
port

shelf  id  remote-port  remote-device
-----  --
3.20  0   Ethernet1/5  S1
3.20  1   -           -
3.20  2   Ethernet1/6  S1
3.20  3   -           -
3.30  0   Ethernet1/7  S1
3.20  1   -           -
3.30  2   Ethernet1/8  S1
3.20  3   -           -
```

2. Retire todos los cables conectados al interruptor de almacenamiento S2.
3. Vuelva a conectar todos los cables al interruptor de repuesto NS2.

Paso 3: Verifique todas las configuraciones de los dispositivos en el switch NS2

1. Verifique el estado de salud de los puertos del nodo de almacenamiento:

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

Mostrar ejemplo

```
storage::*> storage port show -port-type ENET
                                         Speed
VLAN
Node          Port  Type   Mode    (Gb/s)  State   Status
ID
-----
---  
node1
30          e3a   ENET   storage  100  enabled  online
30          e3b   ENET   storage   0  enabled  offline
30          e7a   ENET   storage   0  enabled  offline
30          e7b   ENET   storage  100  enabled  online
node2
30          e3a   ENET   storage  100  enabled  online
30          e3b   ENET   storage   0  enabled  offline
30          e7a   ENET   storage   0  enabled  offline
30          e7b   ENET   storage  100  enabled  online
```

2. Verifique que ambos interruptores estén disponibles:

```
network device-discovery show
```

Mostrar ejemplo

```
storage::*# network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----
node1/cdp
    e3a    S1                      Ethernet1/1
NX3232C
    e4a    node2                  e4a          AFF-
A700
    e4e    node2                  e4e          AFF-
A700
    e7b    NS2                      Ethernet1/1
NX3232C
node1/lldp
    e3a    S1                      Ethernet1/1  -
    e4a    node2                  e4a          -
    e4e    node2                  e4e          -
    e7b    NS2                      Ethernet1/1  -
node2/cdp
    e3a    S1                      Ethernet1/2
NX3232C
    e4a    node1                  e4a          AFF-
A700
    e4e    node1                  e4e          AFF-
A700
    e7b    NS2                      Ethernet1/2
NX3232C
node2/lldp
    e3a    S1                      Ethernet1/2  -
    e4a    node1                  e4a          -
    e4e    node1                  e4e          -
    e7b    NS2                      Ethernet1/2  -
```

3. Verifique los puertos de los estantes en el sistema de almacenamiento:

```
storage shelf port show -fields remote-device,remote-port
```

Mostrar ejemplo

```
storage::*> storage shelf port show -fields remote-device,remote-
port
shelf id remote-port remote-device
-----
3.20 0 Ethernet1/5 S1
3.20 1 Ethernet1/5 NS2
3.20 2 Ethernet1/6 S1
3.20 3 Ethernet1/6 NS2
3.30 0 Ethernet1/7 S1
3.20 1 Ethernet1/7 NS2
3.30 2 Ethernet1/8 S1
3.20 3 Ethernet1/8 NS2
```

4. Si desactivaste la creación automática de casos, vuelve a activarla mediante un mensaje de AutoSupport :

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

¿Que sigue?

Después de sustituir el interruptor, puedes ["configurar la monitorización del estado del comutador"](#).

Actualizar un switch de almacenamiento Cisco Nexus 3232C

Siga estos pasos para actualizar el software Cisco NX-OS y los archivos de configuración de referencia (RCF) en los switches Cisco Nexus 3232C.

Requisitos de revisión

Antes de empezar

Asegúrese de que se cumplan las siguientes condiciones antes de actualizar el software NX-OS y los RCF en el switch de almacenamiento:

- El switch funciona correctamente (no debería haber errores en los registros ni problemas similares).
- Si solo va a instalar NX-OS y a mantener su versión actual de RCF, habrá comprobado o configurado las variables de arranque deseadas en el RCF para que reflejen las imágenes de arranque deseadas.

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

- Ha consultado las guías de software y actualización correspondientes disponibles en la página ["Switches Cisco Nexus serie 3000"](#) para la documentación completa sobre los procedimientos de actualización y degradación del almacenamiento de Cisco.
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la página ["Switches Ethernet Cisco®"](#).

Reemplace el interruptor

Acerca de los ejemplos

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

- Los nombres de los dos comutadores de almacenamiento son S1 y S2.
- Los nodos son nodo1 y nodo2.

Los ejemplos de este procedimiento utilizan dos nodos: el nodo 1 con dos puertos de almacenamiento y el nodo 2 con dos puertos de almacenamiento. Ver el "[Hardware Universe](#)" para verificar los puertos de almacenamiento correctos en sus plataformas. Ver "[¿Qué información adicional necesito para instalar mi equipo que no está en HWU?](#)" para obtener más información sobre los requisitos de instalación del comutador.

 El procedimiento requiere el uso de comandos ONTAP y comandos de switches Cisco Nexus serie 3000; se utilizan comandos ONTAP a menos que se indique lo contrario. Los resultados del comando pueden variar dependiendo de las diferentes versiones de ONTAP.

Paso 1: Compruebe el estado de salud de los comutadores y puertos.

1. Si AutoSupport está habilitado, suprime la creación automática de casos mediante la invocación de un mensaje de AutoSupport :

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

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. Compruebe que los comutadores de almacenamiento estén disponibles:

```
system switch ethernet show
```

Mostrar ejemplo

```
storage::*> system switch ethernet show
Switch          Type          Address
Model
-----
-----
S1          storage-network  172.17.227.5
NX3232C
  Serial Number: FOC221206C2
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
  9.3(3)
  Version Source: CDP

S2          storage-network  172.17.227.6
NX3232C
  Serial Number: FOC220443LZ
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
  9.3(3)
  Version Source: CDP

2 entries were displayed.
storage::*>
```

3. Verifique que los puertos del nodo estén en buen estado y operativos:

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

Mostrar ejemplo

```
storage::*> storage port show -port-type ENET
                                         Speed
VLAN
Node          Port Type  Mode    (Gb/s) State  Status
ID
-----
-----
node1
30          e3a    ENET  storage  100  enabled  online
30          e3b    ENET  storage   0  enabled  offline
30          e7a    ENET  storage   0  enabled  offline
30          e7b    ENET  storage  100  enabled  online
node2
30          e3a    ENET  storage  100  enabled  online
30          e3b    ENET  storage   0  enabled  offline
30          e7a    ENET  storage   0  enabled  offline
30          e7b    ENET  storage  100  enabled  online
30
```

4. Compruebe que no haya problemas con el conmutador de almacenamiento o el cableado:

```
system health alert show -instance
```

Mostrar ejemplo

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

Paso 2: Copie el RCF al switch Cisco S2

1. Copie el RCF del switch S2 a la memoria flash de arranque del switch utilizando uno de los siguientes protocolos de transferencia: FTP, HTTP, TFTP, SFTP o SCP.

Para obtener más información sobre los comandos de Cisco, consulta la guía correspondiente en el ["Referencias de comandos de Cisco Nexus serie 3000 NX-OS"](#).

Mostrar ejemplo

El siguiente ejemplo muestra cómo se utiliza HTTP para copiar un RCF a la memoria flash de arranque del switch S2:

```
S2# copy http://172.16.10.1//cfg/Nexus_3232C_RCF_v1.6-Storage.txt
bootflash: vrf management
% Total      % Received % Xferd  Average Speed   Time     Time
Time                                         Current
                                                Dload  Upload Total Spent
Left
                                                Speed
 100          3254      100      3254      0       0      8175      0
---:---:--- ---:---:--- ---:---:--- 8301
Copy complete, now saving to disk (please wait)...
Copy complete.
S2#
```

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

```
copy bootflash:
```

Mostrar ejemplo

El siguiente ejemplo muestra el archivo RCF. Nexus_3232C_RCF_v1.6-Storage.txt Se está instalando en el switch S2:

```
S2# copy Nexus_3232C_RCF_v1.6-Storage.txt running-config echo-
commands
```

3. 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.



En la salida del banner del show banner motd Para ejecutar este comando, debe leer y seguir las instrucciones de la sección **NOTAS IMPORTANTES** para garantizar la configuración y el funcionamiento correctos del comutador.

+

.Mostrar ejemplo

```
S2# show banner motd

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

S2#

+



Al aplicar RCF por primera vez, el mensaje **ERROR: Failed to write VSH commands** es normal y puede ignorarse.

4. Después de verificar que las versiones del software y la configuración del interruptor sean correctas, copie el running-config archivo al startup-config archivo en el switch S2.

Para obtener más información sobre los comandos de Cisco, consulta la guía correspondiente en el "["Referencias de comandos de Cisco Nexus serie 3000 NX-OS"](#)".

Mostrar ejemplo

El siguiente ejemplo muestra el running-config archivo copiado correctamente al startup-config archivo:

```
S2# copy running-config startup-config
[#####] 100% Copy complete.
```

Paso 3: Copie la imagen de NX-OS al switch Cisco S2 y reinícielo.

1. Copie la imagen NX-OS al switch S2.

Mostrar ejemplo

```
S2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.4.bin /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

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

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

2. Instale la imagen del sistema para que la nueva versión se cargue la próxima vez que se reinicie el switch S2.

El switch se reiniciará en 10 segundos con la nueva imagen, tal como se muestra en la siguiente salida:

Mostrar ejemplo

```
S2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

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

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

Images will be upgraded according to following table:
Module          Image          Running-Version(pri:alt)
New-Version    Upg-Required
-----  -----
-----  -----
          1      nxos          9.3(3)
9.3(4)        yes
          1      bios          v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)        no

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

```
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.  
S2#
```

3. Guarde la configuración.

Para obtener más información sobre los comandos de Cisco, consulta la guía correspondiente en el "["Referencias de comandos de Cisco Nexus serie 3000 NX-OS"](#)".

Se le solicita que reinicie el sistema.

Mostrar ejemplo

```
S2# copy running-config startup-config  
[] 100% Copy complete.  
S2# reload  
This command will reboot the system. (y/n)? [n] y
```

4. Confirme que el número de versión de la nueva versión de NX-OS está en el switch:

Mostrar ejemplo

```
S2# 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/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 Nexus3000 C3232C Chassis (Nexus 9000 Series)
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.

Processor Board ID FOC20291J6K
```

```
Device name: S2
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 due to upgrade

System version: 9.3(3)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

S2#

Paso 4: Vuelva a comprobar el estado de salud de los commutadores y puertos.

1. Vuelva a comprobar que los commutadores de almacenamiento estén disponibles después del reinicio:

```
system switch ethernet show
```

Mostrar ejemplo

```
storage::*> system switch ethernet show
Switch          Type          Address
Model
-----
-----
S1          storage-network  172.17.227.5
NX3232C
  Serial Number: FOC221206C2
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
  9.3(4)
  Version Source: CDP

S2          storage-network  172.17.227.6
NX3232C
  Serial Number: FOC220443LZ
  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.
storage::*>
```

2. Verifique que los puertos del switch estén en buen estado y operativos después del reinicio:

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

Mostrar ejemplo

```
storage::*> storage port show -port-type ENET
                                         Speed
VLAN
Node          Port Type  Mode      (Gb/s) State    Status
ID
-----
-----
node1
30          e3a    ENET  storage    100  enabled  online
30          e3b    ENET  storage      0  enabled  offline
30          e7a    ENET  storage      0  enabled  offline
30          e7b    ENET  storage    100  enabled  online
node2
30          e3a    ENET  storage    100  enabled  online
30          e3b    ENET  storage      0  enabled  offline
30          e7a    ENET  storage      0  enabled  offline
30          e7b    ENET  storage    100  enabled  online
30
```

3. Verifique nuevamente que no haya problemas con el conmutador de almacenamiento o el cableado del clúster:

```
system health alert show -instance
```

Mostrar ejemplo

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

4. Repita el procedimiento para actualizar el software NX-OS y RCF en el switch S1.
5. Si desactivaste la creación automática de casos, vuelve a activarla mediante un mensaje de AutoSupport :

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

¿Que sigue?

Después de actualizar tu switch, puedes ["configurar la monitorización del estado del conmutador"](#).

NVIDIA SN2100

Empezar

Flujo de trabajo de instalación y configuración para conmutadores NVIDIA SN2100

El NVIDIA SN2100 es un switch Ethernet que permite intercambiar datos entre controladores y gabinetes de discos.

Siga estos pasos de flujo de trabajo para instalar y configurar sus conmutadores SN2100.

1

["Revisar los requisitos de configuración"](#)

Revise los requisitos de configuración para el conmutador de almacenamiento SN2100.

2

["Revise los componentes y números de pieza"](#)

Revise los componentes y números de pieza del conmutador de almacenamiento SN2100.

3

["Revisar la documentación requerida"](#)

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores SN2100 y el clúster ONTAP .

4

["Instala el hardware"](#)

Instale el hardware del interruptor.

5

["Configurar el software"](#)

Configurar el software del conmutador.

Requisitos de configuración para los switches NVIDIA SN2100

Para la instalación y el mantenimiento del switch NVIDIA SN2100, asegúrese de revisar todos los requisitos.

Requisitos de instalación

Si desea crear clústeres ONTAP con más de dos nodos, necesitará dos conmutadores de red de clúster compatibles. Puede utilizar interruptores de administración adicionales, que son opcionales.

Instale el conmutador NVIDIA SN2100 (X190006/X190106) en el gabinete de conmutadores dobles/simples de NVIDIA con los soportes estándar que se incluyen con el conmutador.

Para obtener instrucciones sobre el cableado, consulte "["Consideraciones sobre el cableado y la configuración"](#)"

Soporte ONTAP y Linux

El switch NVIDIA SN2100 es un switch Ethernet de 10/25/40/100 Gb que ejecuta Cumulus Linux. El conmutador admite lo siguiente:

- ONTAP 9.10.1P3. El switch SN2100 da servicio a aplicaciones de clúster y almacenamiento en ONTAP 9.10.1P3 a través de diferentes pares de switches. A partir de ONTAP 9.10.1P3, puede usar conmutadores NVIDIA SN2100 para combinar la funcionalidad de almacenamiento y clúster en una configuración de conmutador compartido.
- Sistema operativo Cumulus Linux (CL) versión 4.4.3. Para obtener información actualizada sobre compatibilidad, consulte la "["Commutadores Ethernet NVIDIA"](#) Página informativa.
- Puedes instalar Cumulus Linux cuando el switch esté ejecutando Cumulus Linux u ONIE.

¿Qué sigue?

Después de revisar los requisitos de configuración, puede confirmar su "["componentes y números de pieza"](#)".

Componentes y números de pieza para los interruptores NVIDIA SN2100

Para la instalación y el mantenimiento del switch NVIDIA SN2100, asegúrese de revisar la lista de componentes y números de pieza del kit de gabinete y riel.

Detalles del gabinete

Instale el conmutador NVIDIA SN2100 (X190006/X190106) en el gabinete de conmutadores dobles/simples de NVIDIA con los soportes estándar que se incluyen con el conmutador.

Detalles del kit de rieles

La siguiente tabla enumera el número de pieza y la descripción de los kits de interruptores y rieles MSN2100:

Número de pieza	Descripción
X190006-PE	Conmutador de clúster, NVIDIA SN2100, 16PT 100G, PTSX
X190006-PI	Conmutador de clúster, NVIDIA SN2100, 16PT 100G, PSIN
X190106-FE-PE	Conmutador, NVIDIA SN2100, 16PT 100G, PTSX, Front End
X190106-FE-PI	Conmutador, NVIDIA SN2100, 16PT 100G, PSIN, Front End
X-MTEF-KIT-D	Kit de rieles, interruptor doble NVIDIA lado a lado
X-MTEF-KIT-E	Kit de rieles, interruptor único NVIDIA de profundidad corta



Consulte la documentación de NVIDIA para obtener más detalles sobre "["Instalación del kit de interruptor y riel SN2100"](#)".

¿Qué sigue?

Una vez que haya confirmado sus componentes y números de pieza, puede revisar el ["documentación requerida"](#).

Requisitos de documentación para los conmutadores NVIDIA SN2100

Para la instalación y el mantenimiento del switch NVIDIA SN2100, asegúrese de revisar toda la documentación recomendada.

La siguiente tabla enumera la documentación disponible para los switches NVIDIA SN2100.

Título	Descripción
"Configuración y puesta en marcha de los switches NVIDIA SN2100"	Describe cómo configurar sus switches NVIDIA SN2100, incluyendo la instalación de Cumulus Linux y los RCF aplicables.
"Migrar de un conmutador de almacenamiento Cisco a un conmutador de almacenamiento NVIDIA SN2100"	Describe cómo migrar desde entornos que utilizan conmutadores de almacenamiento Cisco a entornos que utilizan conmutadores de almacenamiento NVIDIA SN2100.
"Migrar a un clúster conmutado de dos nodos con conmutadores de clúster NVIDIA SN2100"	Describe cómo migrar a un entorno conmutado de dos nodos utilizando conmutadores de clúster NVIDIA SN2100.
"Reemplazar un conmutador de almacenamiento NVIDIA SN2100"	Describe el procedimiento para reemplazar un conmutador de almacenamiento NVIDIA SN2100 defectuoso y descargar Cumulus Linux y el archivo de configuración de referencia.

Instalar hardware

Flujo de trabajo de instalación de hardware para conmutadores de almacenamiento NVIDIA SN2100

Para instalar y configurar el hardware de un conmutador de almacenamiento SN2100, siga estos pasos:

1

["Instala el hardware"](#)

Instale el hardware del interruptor.

2

["Revisar las consideraciones de cableado y configuración"](#)

Revisar los requisitos para las conexiones ópticas, el adaptador QSA y la velocidad del puerto de conmutación.

3

["Cablear los estantes NS224"](#)

Siga los procedimientos de cableado si tiene un sistema en el que los estantes de unidades NS224 deben

cablearse como almacenamiento conectado a un comutador (no como almacenamiento de conexión directa).

Instale el hardware para el comutador NVIDIA SN2100.

Para instalar el hardware SN2100, consulte la documentación de NVIDIA.

Pasos

1. Revisar el "[requisitos de configuración](#)" .
2. Siga las instrucciones en "[Guía de instalación de switches NVIDIA](#)" .

¿Que sigue?

Una vez que hayas instalado el hardware, podrás "[revisar el cableado y la configuración](#)" requisitos.

Revisar las consideraciones de cableado y configuración

Antes de configurar su switch NVIDIA SN2100, revise las siguientes consideraciones.

Detalles del puerto NVIDIA

Comutar puertos	Uso de puertos
swp1s0-3	4 nodos de puerto de clúster de ruptura 10GbE
swp2s0-3	4 nodos de puerto de clúster de ruptura de 25 GbE
swp3-14	nodos de puerto de clúster 40/100GbE
swp15-16	Puertos de enlace entre comutadores (ISL) de 100 GbE

Ver el "[Hardware Universe](#)" Para obtener más información sobre los puertos del switch.

Retrasos en la conexión con conexiones ópticas

Si experimenta retrasos de conexión superiores a cinco segundos, Cumulus Linux 5.4 y versiones posteriores incluyen soporte para conexión rápida. Puedes configurar los enlaces utilizando el `nv set` El comando es el siguiente:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Mostrar ejemplo

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Compatibilidad con conexiones de cobre

Para solucionar este problema, son necesarios los siguientes cambios de configuración.

Cumulus Linux 4.4.3

1. Identifique el nombre de cada interfaz que utilice cables de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables

Interface Identifier Vendor Name Vendor PN Vendor SN
Vendor Rev
-----
-----
swp3      0x11 (QSFP28) Molex      112-00576 93A2229911111
B0
swp4      0x11 (QSFP28) Molex      112-00576 93A2229922222
B0
```

2. Agrega las siguientes dos líneas a la /etc/cumulus/switchd.conf archivo para cada puerto (swp<n>) que utilice cables de cobre 40GbE/100GbE:

- interface.swp<n>.enable_media depended_linkup_flow=TRUE
- interface.swp<n>.enable_short_tuning=TRUE

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
.
.
interface.swp3.enable_media depended_linkup_flow=TRUE
interface.swp3.enable_short_tuning=TRUE
interface.swp4.enable_media depended_linkup_flow=TRUE
interface.swp4.enable_short_tuning=TRUE
```

3. Reinicia el switchd servicio:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Confirma que los puertos están activos:

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp3	100G	9216	Trunk/L2		Master:
	bridge (UP)					
UP	swp4	100G	9216	Trunk/L2		Master:
	bridge (UP)					

Cumulus Linux 5.x

1. Identifique el nombre de cada interfaz que utilice cables de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ nv show interface pluggables
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor SN
Vendor	Rev			
swp3	0x11 (QSFP28)	Molex	112-00576	93A2229911111
B0				
swp4	0x11 (QSFP28)	Molex	112-00576	93A2229922222
B0				

2. Configure los enlaces utilizando el `nv set` El comando es el siguiente:

- `nv set interface <interface-id> link fast-linkup on`
- `nv config apply`
- Recarga el `switchd` servicio

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change
```

```
Are you sure? [y/N] y
applied [rev_id: 22]
```

```
Only switchd reload required
```

3. Confirma que los puertos están activos:

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp3	100G	9216	Trunk/L2		Master: bridge (UP)
UP	swp4	100G	9216	Trunk/L2		Master: bridge (UP)

Consulte el artículo de la base de conocimientos "[El switch SN2100 no se conecta usando cables de cobre 40/100GbE.](#)" Para obtener más detalles.

En Cumulus Linux 4.4.2, las conexiones de cobre no son compatibles con los switches SN2100 con NIC X1151A, NIC X1146A o puertos 100GbE integrados. Por ejemplo:

- AFF A800 en los puertos e0a y e0b
- AFF A320 en los puertos e0g y e0h

Adaptador QSA

Cuando se utiliza un adaptador QSA para conectarse a los puertos del clúster 10GbE/25GbE en una plataforma, es posible que el enlace no se establezca.

Para resolver este problema, haga lo siguiente:

- Para 10GbE, configure manualmente la velocidad del enlace swp1s0-3 en 10000 y desactive la negociación automática.
- Para 25GbE, configure manualmente la velocidad del enlace swp2s0-3 en 25000 y desactive la negociación automática.



Cuando utilice adaptadores QSA de 10GbE/25GbE, insértelos en puertos 40GbE/100GbE sin breakout (swp3-swp14). No inserte el adaptador QSA en un puerto configurado para breakout.

Configure la velocidad de la interfaz en los puertos de conexión.

Dependiendo del transceptor en el puerto del switch, es posible que deba configurar la velocidad en la interfaz del switch a una velocidad fija. Si utiliza puertos breakout de 10GbE y 25GbE, verifique que la negociación automática esté desactivada y configure la velocidad de la interfaz en el switch.

Cumulus Linux 4.4.3

Por ejemplo:

```
cumulus@cumulus:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces      2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp 2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
      alias 10G Intra-Cluster Node
      link-autoneg off
      link-speed 10000 <---- port speed set
      mstpctl-bpduguard yes
      mstpctl-portadminedge yes
      mtu 9216

auto swp1s3
iface swp1s3
      alias 10G Intra-Cluster Node
      - link-autoneg off
      + link-autoneg on
      link-speed 10000 <---- port speed set
      mstpctl-bpduguard yes
      mstpctl-portadminedge yes
      mtu 9216

auto swp2s0
iface swp2s0
      alias 25G Intra-Cluster Node
      link-autoneg off
      link-speed 25000 <---- port speed set
```

Compruebe el estado de la interfaz y del puerto para verificar que la configuración se haya aplicado:

```
cumulus@cumulus:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
<hr/>						
<hr/>						
<hr/>						
.						
.						
UP	swp1s0	10G	9216	Trunk/L2	cs07 (e4c)	Master:
br_default(UP)						
UP	swp1s1	10G	9216	Trunk/L2	cs07 (e4d)	Master:
br_default(UP)						
UP	swp1s2	10G	9216	Trunk/L2	cs08 (e4c)	Master:
br_default(UP)						
UP	swp1s3	10G	9216	Trunk/L2	cs08 (e4d)	Master:
br_default(UP)						
.						
.						
UP	swp3	40G	9216	Trunk/L2	cs03 (e4e)	Master:
br_default(UP)						
UP	swp4	40G	9216	Trunk/L2	cs04 (e4e)	Master:
br_default(UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
br_default(UP)						
.						
.						
UP	swp15	100G	9216	BondMember	cs01 (swp15)	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	cs01 (swp16)	Master:
cluster_isl(UP)						
.						
.						

Cumulus Linux 5.x

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3

link

  auto-negotiate      off          off
  off
  duplex              full         full
  full
  speed               10G         10G
  10G
  fec                 auto         auto
  auto
  mtu                9216        9216
  9216
  [breakout]

  state              up          up
  up
```

Compruebe el estado de la interfaz y del puerto para verificar que la configuración se haya aplicado:

```
cumulus@cumulus:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
<hr/>						
<hr/>						
<hr/>						
.						
.						
UP	swp1s0	10G	9216	Trunk/L2	cs07 (e4c)	Master:
br_default(UP)						
UP	swp1s1	10G	9216	Trunk/L2	cs07 (e4d)	Master:
br_default(UP)						
UP	swp1s2	10G	9216	Trunk/L2	cs08 (e4c)	Master:
br_default(UP)						
UP	swp1s3	10G	9216	Trunk/L2	cs08 (e4d)	Master:
br_default(UP)						
.						
.						
UP	swp3	40G	9216	Trunk/L2	cs03 (e4e)	Master:
br_default(UP)						
UP	swp4	40G	9216	Trunk/L2	cs04 (e4e)	Master:
br_default(UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
br_default(UP)						
.						
.						
UP	swp15	100G	9216	BondMember	cs01 (swp15)	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	cs01 (swp16)	Master:
cluster_isl(UP)						
.						
.						

¿Que sigue?

Después de revisar los requisitos de cableado y configuración, puedes ["Cablee los estantes NS224 como almacenamiento conectado al interruptor."](#)

Estanterías Cable NS224 como almacenamiento conectado al interruptor

Si tiene un sistema en el que los estantes de unidades NS224 deben cablearse como almacenamiento conectado a un commutador (no como almacenamiento conectado directamente), utilice la información proporcionada aquí.

- Cable NS224 estantes de unidades a través de conmutadores de almacenamiento:
["Información para el cableado de los bastidores de unidades NS224 conectados al conmutador."](#)
- Instala tus conmutadores de almacenamiento:
["Documentación de los conmutadores AFF y FAS"](#)
- Confirme el hardware compatible, como conmutadores de almacenamiento y cables, para su modelo de plataforma:
["NetApp Hardware Universe"](#)

Configurar software

Flujo de trabajo de instalación de software para conmutadores de almacenamiento NVIDIA SN2100

Para instalar y configurar el software para un switch NVIDIA SN2100, siga estos pasos:

1

["Configura el interruptor"](#)

Configurar el conmutador NVIDIA SN2100.

2

["Instalar Cumulus Linux en modo Cumulus"](#)

Puede instalar el sistema operativo Cumulus Linux (CL) cuando el conmutador ejecuta Cumulus Linux.

3

["Instalar Cumulus Linux en modo ONIE"](#)

Como alternativa, puede instalar el sistema operativo Cumulus Linux (CL) cuando el conmutador ejecuta Cumulus Linux en modo ONIE.

4

["Instalar el script del archivo de configuración de referencia \(RCF\)"](#)

Existen dos scripts RCF disponibles para aplicaciones de Clustering y Almacenamiento. El procedimiento es el mismo para cada uno.

5

["Instala el archivo CSHM"](#)

Puede instalar el archivo de configuración correspondiente para la monitorización del estado de los switches Ethernet de los clústeres NVIDIA .

6

["Restablecer el interruptor a los valores predeterminados de fábrica"](#)

Borre la configuración del interruptor de almacenamiento SN2100.

Configure el conmutador NVIDIA SN2100

Para configurar el switch SN2100, consulte la documentación de NVIDIA.

Pasos

1. Revisar el "[requisitos de configuración](#)" .
2. Siga las instrucciones en "[Puesta en marcha del sistema NVIDIA](#) ."

¿Que sigue?

Una vez que hayas configurado tus interruptores, podrás "[Instalar Cumulus Linux en modo Cumulus](#)" o "[Instalar Cumulus Linux en modo ONIE](#)" .

Instalar Cumulus Linux en modo Cumulus

Siga este procedimiento para instalar el sistema operativo Cumulus Linux (CL) cuando el switch esté funcionando en modo Cumulus.



El sistema operativo Cumulus Linux (CL) se puede instalar cuando el switch ejecuta Cumulus Linux u ONIE (véase "[Instalar en modo ONIE](#)").

Antes de empezar

Asegúrese de que esté disponible lo siguiente:

- Conocimientos de Linux de nivel intermedio.
- Conocimientos básicos de edición de texto, permisos de archivos UNIX y monitorización de procesos. Se incluyen varios editores de texto preinstalados, entre ellos: `vi` y `nano` .
- Acceso a una consola Linux o UNIX. Si utiliza Windows, use un entorno Linux como herramienta de línea de comandos para interactuar con Cumulus Linux.
- La velocidad de transmisión debe configurarse en 115200 en el conmutador de consola serie para el acceso a la consola del conmutador NVIDIA SN2100, como se indica a continuación:
 - 115200 baudios
 - 8 bits de datos
 - 1 bit de parada
 - paridad: ninguna
 - Control de flujo: ninguno

Acerca de esta tarea

Tenga en cuenta lo siguiente:



Cada vez que se instala Cumulus Linux, se borra y se reconstruye toda la estructura del sistema de archivos.



La contraseña predeterminada para la cuenta de usuario `cumulus` es **cumulus**. La primera vez que inicie sesión en Cumulus Linux, deberá cambiar esta contraseña predeterminada. Asegúrese de actualizar cualquier script de automatización antes de instalar una nueva imagen. Cumulus Linux proporciona opciones de línea de comandos para cambiar automáticamente la contraseña predeterminada durante el proceso de instalación.

Ejemplo 1. Pasos

Cumulus Linux 4.4.3

1. Inicia sesión en el switch.

El primer inicio de sesión en el switch requiere el nombre de usuario/contraseña **cumulus/cumulus** con sudo privilegios.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Comprueba la versión de Cumulus para Linux: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo surtirá efecto después de reiniciar la sesión de consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz está diseñada específicamente para su uso en la gestión fuera de banda. Por defecto, la interfaz de administración utiliza DHCPv4 para el direccionamiento.



No utilice guiones bajos (_), apóstrofes (') ni caracteres no ASCII en el nombre de host.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Este comando modifica ambos /etc/hostname y /etc/hosts archivos.

4. Confirme que el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada se han actualizado.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0  device
memory 0xdxfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Configure la fecha, la hora, la zona horaria y el servidor NTP en el conmutador.

- Verifique la zona horaria actual:

```
cumulus@sw1:~$ cat /etc/timezone
```

- Actualización a la nueva zona horaria:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive  
tzdata
```

c. Verifique su zona horaria actual:

```
cumulus@switch:~$ date +%Z
```

d. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Configure el reloj del software según la zona horaria configurada:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Establezca el valor actual del reloj del software al del reloj del hardware:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>  
iburst  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

h. Verifique que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp  
ntp      4074      1  0 Jun20 ?          00:00:33 /usr/sbin/ntpd -p  
/var/run/ntpd.pid -g -u 101:102
```

i. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que utiliza NTP es eth0 . Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ net add time ntp source <src_int>  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

6. Instalar Cumulus Linux 4.4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones en la pantalla de GRUB. No realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar sistema operativo
- INSTALACIÓN DE CÚMULOS
- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Verifique que la versión de Cumulus Linux sea la 4.4.3: `net show version`

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Crea un nuevo usuario y agrégalo a la lista. `sudo grupo`. Este usuario solo será efectivo después de reiniciar la sesión de consola/SSH.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
```

```
cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.
```

```
[admin@cycrh6sv101 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1ul
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)
```

For support and online technical documentation, visit
<http://www.cumulusnetworks.com/support>

The registered trademark Linux (R) is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

```
admin@sw1:mgmt:~$
```

Cumulus Linux 5.4.0

1. Inicia sesión en el switch.

El primer inicio de sesión en el switch requiere el nombre de usuario/contraseña **cumulus/cumulus**

con sudo privilegios.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Comprueba la versión de Cumulus para Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational      applied      description
-----
hostname         cumulus      cumulus
build            Cumulus Linux 5.3.0  system build version
uptime           6 days, 8:37:36  system uptime
timezone         Etc/UTC      system time zone
```

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo surtirá efecto después de reiniciar la sesión de consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz está diseñada específicamente para su uso en la gestión fuera de banda. Por defecto, la interfaz de administración utiliza DHCPv4 para el direccionamiento.



No utilice guiones bajos (`_`), apóstrofes (`'`) ni caracteres no ASCII en el nombre de host.

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica ambos `/etc/hostname` y `/etc/hosts` archivos.

4. Confirme que el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace

predeterminada se han actualizado.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Configure la zona horaria, la fecha, la hora y el servidor NTP en el conmutador.

a. Configura la zona horaria:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

b. Verifique su zona horaria actual:

```
cumulus@switch:~$ date +%Z
```

c. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

d. Configure el reloj del software según la zona horaria configurada:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

e. Establezca el valor actual del reloj del software al del reloj del hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Consulte el artículo de la base de conocimientos "["La configuración del servidor NTP no funciona con los switches NVIDIA SN2100."](#)" Para obtener más detalles.

g. Verifique que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp      4074      1  0 Jun20 ?          00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que utiliza NTP es eth0 . Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instalar Cumulus Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones en la pantalla de GRUB. No realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar sistema operativo
- INSTALACIÓN DE CÚMULOS

- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Verifique que la versión de Cumulus Linux sea la 5.4.0: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational           applied           description
-----
hostname              cumulus           cumulus
build                 Cumulus Linux 5.4.0  system build version
uptime                6 days, 13:37:36  system uptime
timezone              Etc/UTC           system time zone
```

11. Verifique que cada nodo tenga conexión con cada conmutador:

```
cumulus@sw1:mgmt:~$ net show lldp

LocalPort  Speed  Mode          RemoteHost
RemotePort

-----
-----
eth0       100M   Mgmt         mgmt-sw1
Eth110/1/29
swp2s1     25G    Trunk/L2    node1
e0a
swp15      100G   BondMember  sw2
swp15
swp16      100G   BondMember  sw2
swp16
```

12. Crea un nuevo usuario y agrégalo a la lista `sudo` grupo. Este usuario solo será efectivo después de reiniciar la sesión de consola/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6sv101 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

13. Agregue grupos de usuarios adicionales para que el usuario administrador pueda acceder a ellos. **nv** comandos:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user 'admin' to group 'nvshow' ...
Adding user admin to group nvshow
Done.
```

Ver "[Cuentas de usuario de NVIDIA](#)" Para más información.

Cumulus Linux 5.11.0

1. Inicia sesión en el switch.

Cuando inicie sesión en el switch por primera vez, le solicitará el nombre de usuario y la contraseña **cumulus/cumulus** con `sudo` privilegios.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Comprueba la versión de Cumulus para Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational      applied          description
-----
hostname          cumulus          cumulus
build             Cumulus Linux 5.4.0  system build version
uptime            6 days, 8:37:36    system uptime
timezone          Etc/UTC          system time zone
```

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo surtirá efecto después de reiniciar la sesión de consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz está diseñada específicamente para su uso en la gestión fuera de banda. Por defecto, la interfaz de administración utiliza DHCPv4 para el direccionamiento.



No utilice guiones bajos (`_`), apóstrofes (`'`) ni caracteres no ASCII en el nombre de host.

```

cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save

```

Este comando modifica ambos /etc/hostname y /etc/hosts archivos.

4. Confirme que el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada se han actualizado.

```

cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdxfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1

```

5. Configure la zona horaria, la fecha, la hora y el servidor NTP en el conmutador.

- a. Configura la zona horaria:

```

cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply

```

- b. Verifique su zona horaria actual:

```

cumulus@switch:~$ date +%Z

```

- c. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

- d. Configure el reloj del software según la zona horaria configurada:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

- e. Establezca el valor actual del reloj del software al del reloj del hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

- f. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Consulte el artículo de la base de conocimientos "["La configuración del servidor NTP no funciona con los switches NVIDIA SN2100."](#) Para obtener más detalles.

- g. Verifique que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp      4074      1  0 Jun20 ?          00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

- h. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que utiliza NTP es eth0. Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instalar Cumulus Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones en la pantalla de GRUB. No realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar sistema operativo
- INSTALACIÓN DE CÚMULOS
- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Verifique que la versión de Cumulus Linux sea la 5.11.0:

```
nv show system
```

```
cumulus@cumulus:mgmt:~$ nv show system
operational           applied           description
-----
build                 Cumulus Linux 5.11.0
uptime                153 days, 2:44:16
hostname              cumulus           cumulus
product-name          Cumulus Linux
product-release       5.11.0
platform              x86_64-mlnx_x86-r0
system-memory         2.76 GB used / 2.28 GB free / 7.47 GB total
swap-memory           0 Bytes used / 0 Bytes free / 0 Bytes total
health-status         not OK
date-time             2025-04-23 09:55:24
status                N/A
timezone              Etc/UTC
maintenance
  mode                disabled
  ports               enabled
version
  kernel              6.1.0-cl-1-amd64
  build-date          Thu Nov 14 13:06:38 UTC 2024
  image               5.11.0
  onie                2019.11-5.2.0020-115200
```

11. Verifique que cada nodo tenga conexión con cada conmutador:

```
cumulus@sw1:mgmt:~$ nv show interface lldp

  LocalPort   Speed   Mode          RemoteHost
  RemotePort
  -----  -----  -----  -----
  -----
  eth0      100M   eth    mgmt-sw1
  Eth110/1/14
  swp2s1    25G    Trunk/L2    node1
  e0a
  swp1s1    10G    swp     sw2
  e0a
  swp9      100G   swp     sw3
  e4a
  swp10     100G   swp     sw4
  e4a
  swp15     100G   swp     sw5
  swp15
  swp16     100G   swp     sw6
  swp16
```

Ver "[Cuentas de usuario de NVIDIA](#)" Para más información.

¿Que sigue?

Una vez que hayas instalado Cumulus Linux en modo Cumulus, podrás "[Instalar o actualizar el script RCF](#)" .

Instalar Cumulus Linux en modo ONIE

Siga este procedimiento para instalar el sistema operativo Cumulus Linux (CL) cuando el switch esté funcionando en modo ONIE.



El sistema operativo Cumulus Linux (CL) se puede instalar cuando el switch ejecuta Cumulus Linux u ONIE (véase "[Instalar en modo Cumulus](#)").

Acerca de esta tarea

Puede instalar Cumulus Linux utilizando Open Network Install Environment (ONIE), que permite la detección automática de una imagen de instalación de red. Esto facilita el modelo de sistema para asegurar los switches con una elección de sistema operativo, como Cumulus Linux. La forma más sencilla de instalar Cumulus Linux con ONIE es mediante detección HTTP local.



Si su host tiene habilitado IPv6, asegúrese de que esté ejecutando un servidor web. Si su host está habilitado para IPv4, asegúrese de que esté ejecutando DHCP además de un servidor web.

Este procedimiento muestra cómo actualizar Cumulus Linux después de que el administrador haya arrancado en ONIE.

Pasos

1. Descargue el archivo de instalación de Cumulus Linux al directorio raíz del servidor web. Cambiar el nombre de este archivo **onie-installer** .
2. Conecte su equipo al puerto Ethernet de administración del switch mediante un cable Ethernet.
3. Encienda el interruptor. El switch descarga el instalador de la imagen ONIE y se inicia. Una vez finalizada la instalación, aparece el indicador de inicio de sesión de Cumulus Linux en la ventana de la terminal.



Cada vez que se instala Cumulus Linux, se borra y se reconstruye toda la estructura del sistema de archivos.

4. Reinicie el switch SN2100:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

5. Presione la tecla **Esc** en la pantalla de GNU GRUB para interrumpir el proceso de arranque normal, seleccione **ONIE** y presione **Enter**.
6. En la siguiente pantalla que aparece, seleccione **ONIE: Instalar SO**.
7. El proceso de detección del instalador de ONIE se ejecuta buscando la instalación automática. Pulse **Enter** para detener temporalmente el proceso.
8. Cuando el proceso de descubrimiento se ha detenido:

```
ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover...start-stop-daemon: warning: killing process 427:
No such process done.
```

9. Si el servicio DHCP está en funcionamiento en su red, verifique que la dirección IP, la máscara de subred y la puerta de enlace predeterminada estén asignadas correctamente:

```
ifconfig eth0
```

Mostrar ejemplo

```
ONIE:/ # ifconfig eth0
eth0      Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
          inet  addr:10.233.204.71  Bcast:10.233.205.255
          Mask:255.255.254.0
                  inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                      RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
                      TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
                      Memory:dfc00000-dfc1ffff

ONIE:/ # route
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref
Use  Iface

default        10.233.204.1    0.0.0.0        UG      0      0
0    eth0
10.233.204.0    *              255.255.254.0  U      0      0
0    eth0
```

10. Si el esquema de direccionamiento IP se define manualmente, haga lo siguiente:

```
ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1
```

11. Repita el paso 9 para verificar que la información estática se haya ingresado correctamente.
12. Instalar Cumulus Linux:

```
ONIE:/ # route

Kernel IP routing table

ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-linux-
4.4.3-mlx-amd64.bin

Stopping: discover... done.
Info: Attempting
http://10.60.132.97/x/eng/testbedN,sv1/nic/files/cumulus-linux-4.4.3-
mlx-amd64.bin ...
Connecting to 10.60.132.97 (10.60.132.97:80)
installer          100% |*|    552M  0:00:00 ETA
...
...
```

13. Una vez finalizada la instalación, inicie sesión en el switch:

Mostrar ejemplo

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

14. Verifique la versión de Cumulus para Linux:

```
net show version
```

Mostrar ejemplo

```
cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-c14.4.3u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

¿Que sigue?

Una vez instalado Cumulus Linux en modo ONIE, puedes "[Instalar o actualizar el script RCF](#)".

Instale o actualice el script RCF.

Siga este procedimiento para instalar o actualizar el script RCF.

Antes de empezar

Antes de instalar o actualizar el script RCF, asegúrese de que lo siguiente esté disponible en el switch:

- Está instalado Cumulus Linux 4.4.3.
- Dirección IP, máscara de subred y puerta de enlace predeterminada definidas mediante DHCP o configuradas manualmente.

Versiones actuales del script RCF

Existen dos scripts RCF disponibles para aplicaciones de Clustering y Almacenamiento. El procedimiento es el mismo para cada uno.

- Agrupamiento: **MSN2100-RCF-v1.x-Cluster**
- Almacenamiento: **MSN2100-RCF-v1.x-Almacenamiento**



El siguiente procedimiento de ejemplo muestra cómo descargar y aplicar el script RCF para comutadores de clúster.



La salida del comando de ejemplo utiliza la dirección IP de administración del switch 10.233.204.71, la máscara de red 255.255.254.0 y la puerta de enlace predeterminada 10.233.204.1.

Pasos

1. Muestra las interfaces disponibles en el switch SN2100:

```
net show interface all
```

Mostrar ejemplo

```
cumulus@cumulus:mgmt:~$ net show interface all

  State  Name    Spd   MTU    Mode          LLDP          Summary
-----  -----  ---  -----  -----  -----
-----  ...
...
ADMDN  swp1    N/A  9216  NotConfigured
ADMDN  swp2    N/A  9216  NotConfigured
ADMDN  swp3    N/A  9216  NotConfigured
ADMDN  swp4    N/A  9216  NotConfigured
ADMDN  swp5    N/A  9216  NotConfigured
ADMDN  swp6    N/A  9216  NotConfigured
ADMDN  swp7    N/A  9216  NotConfigured
ADMDN  swp8    N/A  9216  NotConfigured
ADMDN  swp9    N/A  9216  NotConfigured
ADMDN  swp10   N/A  9216  NotConfigured
ADMDN  swp11   N/A  9216  NotConfigured
ADMDN  swp12   N/A  9216  NotConfigured
ADMDN  swp13   N/A  9216  NotConfigured
ADMDN  swp14   N/A  9216  NotConfigured
ADMDN  swp15   N/A  9216  NotConfigured
ADMDN  swp16   N/A  9216  NotConfigured
```

2. Copie el script de Python de RCF al switch:

```
admin@sw1:mgmt:~$ pwd
/home/cumulus
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host>:/<path>/MSN2100-RCF-v1.8-Cluster
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.8-Cluster                                100%  8607    111.2KB/s
00:00
```

3. Aplique el script de Python RCF **MSN2100-RCF-v1.8-Cluster**:

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.8-Cluster
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

El script RCF completa los pasos enumerados anteriormente.



Para cualquier problema con el script de Python de RCF que no se pueda corregir, póngase en contacto con ["Soporte de NetApp"](#) para obtener ayuda.

4. Vuelva a aplicar cualquier personalización anterior a la configuración del switch. Referirse a ["Revisar las consideraciones de cableado y configuración"](#) Para obtener detalles sobre cualquier otro cambio necesario.
5. Verifique la configuración después del reinicio:

```
net show interface all
```

Mostrar ejemplo

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
---	---	---	---	---	---	---
...						
...						
DN	swp1s0 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp1s1 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp1s2 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp1s3 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp2s0 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp2s1 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp2s2 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp2s3 bridge (UP)	N/A	9216	Trunk/L2		Master:
UP	swp3 bridge (UP)	100G	9216	Trunk/L2		Master:
UP	swp4 bridge (UP)	100G	9216	Trunk/L2		Master:
DN	swp5 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp6 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp7 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp8 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp9 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp10 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp11 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp12 bridge (UP)	N/A	9216	Trunk/L2		Master:
DN	swp13 bridge (UP)	N/A	9216	Trunk/L2		Master:

DN	swp14	N/A	9216	Trunk/L2	Master:
bridge (UP)					
UP	swp15	N/A	9216	BondMember	Master:
bond_15_16 (UP)					
UP	swp16	N/A	9216	BondMember	Master:
bond_15_16 (UP)					
...					
...					

```

cumulus@cumulus:mgmt:~$ net show roce config
RoCE mode..... lossless
Congestion Control:
  Enabled SPs.... 0 2 5
  Mode..... ECN
  Min Threshold.. 150 KB
  Max Threshold.. 1500 KB
PFC:
  Status..... enabled
  Enabled SPs.... 2 5
  Interfaces..... swp10-16, swp1s0-3, swp2s0-3, swp3-9

  DSCP          802.1p  switch-priority
  -----        -----  -----
  0 1 2 3 4 5 6 7          0          0
  8 9 10 11 12 13 14 15     1          1
  16 17 18 19 20 21 22 23     2          2
  24 25 26 27 28 29 30 31     3          3
  32 33 34 35 36 37 38 39     4          4
  40 41 42 43 44 45 46 47     5          5
  48 49 50 51 52 53 54 55     6          6
  56 57 58 59 60 61 62 63     7          7

  switch-priority  TC  ETS
  -----  -----  -----
  0 1 3 4 6 7      0  DWRR 28%
  2                  2  DWRR 28%
  5                  5  DWRR 43%

```

6. Verifique la información del transceptor en la interfaz:

```
net show interface pluggables
```

Mostrar ejemplo

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
Interface Identifier      Vendor Name  Vendor PN      Vendor SN
      Vendor Rev
-----
-----
swp3      0x11 (QSFP28)  Amphenol      112-00574
APF20379253516  B0
swp4      0x11 (QSFP28)  AVAGO        332-00440      AF1815GU05Z
      A0
swp15     0x11 (QSFP28)  Amphenol      112-00573
APF21109348001  B0
swp16     0x11 (QSFP28)  Amphenol      112-00573
APF21109347895  B0
```

7. Verifique que cada nodo tenga conexión con cada conmutador:

```
net show lldp
```

Mostrar ejemplo

```
cumulus@cumulus:mgmt:~$ net show lldp
LocalPort  Speed  Mode          RemoteHost      RemotePort
-----
swp3       100G  Trunk/L2      sw1            e3a
swp4       100G  Trunk/L2      sw2            e3b
swp15      100G  BondMember    sw13           swp15
swp16      100G  BondMember    sw14           swp16
```

8. Verifique el estado de los puertos del clúster.

- Verifique que los puertos e0d estén activos y en buen estado en todos los nodos del clúster:

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

Mostrar ejemplo

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

Node: node1

Ignore                                         Speed (Mbps)  Health
Health
Port      IPspace      Broadcast  Domain  Link  MTU  Admin/Oper  Status
Status
-----
-----
e3a      Cluster      Cluster      up      9000  auto/10000
healthy  false
e3b      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
-----
-----
e3a      Cluster      Cluster      up      9000  auto/10000
healthy  false
e3b      Cluster      Cluster      up      9000  auto/10000
healthy  false
```

- a. Verifique el estado del switch desde el clúster (esto podría no mostrar el switch sw2, ya que las LIF no están conectadas a e0d).

Mostrar ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface Platform
-----
node1/lldp
      e3a      sw1 (b8:ce:f6:19:1a:7e)  swp3      -
      e3b      sw2 (b8:ce:f6:19:1b:96)  swp3      -
node2/lldp
      e3a      sw1 (b8:ce:f6:19:1a:7e)  swp4      -
      e3b      sw2 (b8:ce:f6:19:1b:96)  swp4      -

cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                  Type          Address
Model
-----
-----
sw1                    cluster-network 10.233.205.90
MSN2100-CB2RC
  Serial Number: MNXXXXXXGD
  Is Monitored: true
  Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
  Mellanox
  Technologies Ltd. MSN2100
  Version Source: LLDP

sw2                    cluster-network 10.233.205.91
MSN2100-CB2RC
  Serial Number: MNCXXXXXXGS
  Is Monitored: true
  Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
  Mellanox
  Technologies Ltd. MSN2100
  Version Source: LLDP
```

¿Que sigue?

Después de instalar o actualizar RCF, puedes "["Instalar el archivo CSHM"](#) .

Instale el archivo de configuración del monitor de estado del switch Ethernet.

Siga este procedimiento para instalar el archivo de configuración correspondiente para la monitorización del estado de los switches Ethernet de los clústeres NVIDIA. Los modelos compatibles son:

- MSN2100-CB2FC
- MSN2100-CB2RC
- X190006-PE
- X190006-PI



Este procedimiento de instalación se aplica a ONTAP 9.10.1 y versiones posteriores.

Antes de empezar

- Verifique que necesita descargar el archivo de configuración ejecutando `system switch ethernet show` y comprobar si aparece **OTRO** para su modelo.

Si su modelo sigue mostrando **OTRO** después de aplicar el archivo de configuración, póngase en contacto con el soporte de NetApp.

- Asegúrese de que el clúster ONTAP esté en funcionamiento.
- Habilita SSH para utilizar todas las funciones disponibles en CSHM.
- Borrar el `/mroot/etc/cshm_nod/nod_sign/` directorio en todos los nodos:
 - a. Ingrese al nodeshell:

```
system node run -node <name>
```

- b. Cambio a privilegios avanzados:

```
priv set advanced
```

- c. Enumere los archivos de configuración en el `/etc/cshm_nod/nod_sign` directorio. Si el directorio existe y contiene archivos de configuración, muestra una lista con los nombres de los archivos.

```
ls /etc/cshm_nod/nod_sign
```

- d. Elimine todos los archivos de configuración correspondientes a los modelos de interruptores conectados.

Si no está seguro, elimine todos los archivos de configuración de los modelos compatibles enumerados anteriormente y, a continuación, descargue e instale los archivos de configuración más recientes para esos mismos modelos.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

- a. Confirma que los archivos de configuración eliminados ya no se encuentran en el directorio:

```
ls /etc/cshm_nod/nod_sign
```

Pasos

1. Descargue el archivo zip de configuración del monitor de estado del switch Ethernet según la versión de lanzamiento de ONTAP correspondiente. Este archivo está disponible en "[conmutadores Ethernet NVIDIA](#)" página.
 - a. En la página de descarga del software NVIDIA SN2100, seleccione **Archivo Nvidia CSHM**.
 - b. En la página de Precaución/Lectura obligatoria, seleccione la casilla de verificación para estar de acuerdo.
 - c. En la página del Acuerdo de Licencia de Usuario Final, seleccione la casilla de verificación para aceptar y haga clic en **Aceptar y continuar**.
 - d. En la página de descarga de archivos Nvidia CSHM, seleccione el archivo de configuración correspondiente. Los siguientes archivos están disponibles:

ONTAP 9.15.1 y posteriores

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 a 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. Cargue el archivo zip correspondiente a su servidor web interno.
2. Acceda a la configuración del modo avanzado desde uno de los sistemas ONTAP del clúster.

```
set -privilege advanced
```

3. Ejecute el comando de configuración del monitor de estado del switch.

```
cluster1::> system switch ethernet configure-health-monitor
```

4. Verifique que el resultado del comando finalice con el siguiente texto para su versión de ONTAP :

ONTAP 9.15.1 y posteriores

El sistema de monitorización del estado del switch Ethernet instaló el archivo de configuración.

ONTAP 9.11.1 a 9.14.1

SHM instaló el archivo de configuración.

ONTAP 9.10.1

El paquete descargado de CSHM se procesó correctamente.

Si se produce un error, póngase en contacto con el soporte de NetApp .

1. Espere hasta el doble del intervalo de sondeo del monitor de estado del switch Ethernet, que se obtiene ejecutando `system switch ethernet polling-interval show` , antes de completar el siguiente paso.
2. Ejecutar el comando `system switch ethernet configure-health-monitor show` en el sistema ONTAP y asegúrese de que los comutadores del clúster se detecten con el campo monitoreado establecido en **Verdadero** y el campo del número de serie no muestre **Desconocido**.

```
cluster1::> system switch ethernet configure-health-monitor show
```

¿Que sigue?

Después de instalar el archivo CSHM, puedes "[configurar la monitorización del estado del comutador](#)" .

Restablecer el interruptor de almacenamiento SN2100 a los valores predeterminados de fábrica

Para restablecer el interruptor de almacenamiento SN2100 a los valores predeterminados de fábrica:

- Para Cumulus Linux 5.10 y versiones anteriores, aplique la imagen de Cumulus.
- Para Cumulus Linux 5.11 y versiones posteriores, se utiliza el `nv action reset system factory-default dominio`.

Acerca de esta tarea

- Debes estar conectado al switch mediante la consola serie.
- Debe tener la contraseña root para acceder a los comandos de sudo.



Para obtener más información sobre la instalación de Cumulus Linux, consulte "[Flujo de trabajo de instalación de software para switches NVIDIA SN2100](#)" .

Ejemplo 2. Pasos

Cumulus Linux 5.10 y anteriores

1. Desde la consola de Cumulus, descargue y ponga en cola la instalación del software del switch con el comando `onie-install -a -i` seguido de la ruta de acceso al archivo del software del conmutador, por ejemplo:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. El instalador inicia la descarga. Escriba `y` cuando se le solicite para confirmar la instalación cuando se haya descargado y verificado la imagen.
3. Reinicie el conmutador para instalar el nuevo software.

```
sudo reboot
```

```
cumulus@sw1:mgmt:~$ sudo reboot
```



El conmutador se reinicia y accede a la instalación del software del conmutador, lo que lleva algún tiempo. Cuando finaliza la instalación, el switch se reinicia y permanece en el `log-in` inmediato.

Cumulus Linux 5.11 y posteriores

1. Para restablecer el interruptor a los valores predeterminados de fábrica y eliminar toda la configuración, los archivos del sistema y los archivos de registro, ejecute:

```
nv action reset system factory-default
```

Por ejemplo:

```
cumulus@switch:~$ nv action reset system factory-default
```

This operation will reset the system configuration, delete the log files and reboot the switch.

Type [y] continue.

Type [n] to abort.

Do you want to continue? [y/n] **y**

Consulta la página de NVIDIA. "[Restablecimiento de fábrica](#)" Documentación para más detalles.

¿Qué sigue?

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

Migrar interruptores

Migrar de un switch de almacenamiento Cisco a un switch de almacenamiento NVIDIA SN2100

Puede migrar switches Cisco antiguos para un clúster ONTAP a switches de almacenamiento NVIDIA SN2100. Este es un procedimiento que no produce interrupciones.

Requisitos de revisión

Se admiten los siguientes conmutadores de almacenamiento:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- Ver el ["Hardware Universe"](#) Para obtener información detallada sobre los puertos compatibles y sus configuraciones.

Antes de empezar

Asegúrese de tener lo siguiente:

- El clúster existente está configurado y funcionando correctamente.
- Todos los puertos de almacenamiento están en estado activo para garantizar un funcionamiento sin interrupciones.
- Los conmutadores de almacenamiento NVIDIA SN2100 están configurados y funcionando bajo la versión correcta de Cumulus Linux instalada con el archivo de configuración de referencia (RCF) aplicado.
- La configuración de red de almacenamiento existente presenta lo siguiente:
 - Un clúster NetApp redundante y totalmente funcional que utiliza ambos switches Cisco antiguos.
 - Conectividad de gestión y acceso a la consola tanto para los switches Cisco antiguos como para los nuevos.
 - Todas las LIF del clúster en estado activo están en sus puertos de origen.
 - Puertos ISL habilitados y cableados entre los switches Cisco antiguos y entre los switches nuevos.
- Ver el ["Hardware Universe"](#) Para obtener información detallada sobre los puertos compatibles y sus configuraciones.
- Algunos de los puertos están configurados en los switches NVIDIA SN2100 para funcionar a 100 GbE.
- Has planificado, migrado y documentado la conectividad 100 GbE desde los nodos a los conmutadores de almacenamiento NVIDIA SN2100.

Migrar los interruptores

Acerca de los ejemplos

En este procedimiento, se utilizan switches de almacenamiento Cisco Nexus 9336C-FX2 como ejemplos de comandos y salidas.

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

- Los switches de almacenamiento Cisco Nexus 9336C-FX2 existentes son *S1* y *S2*.
- Los nuevos conmutadores de almacenamiento NVIDIA SN2100 son *sw1* y *sw2*.

- Los nodos son *nodo1* y *nodo2*.
- Los LIF del clúster son *node1_clus1* y *node1_clus2* en el nodo 1, y *node2_clus1* y *node2_clus2* en el nodo 2 respectivamente.
- El *cluster1::*>* El indicador muestra el nombre del clúster.
- Los puertos de red utilizados en este procedimiento son *e5a* y *e5b*.
- Los puertos de ruptura adoptan el formato: *swp1s0-3*. Por ejemplo, cuatro puertos de ruptura en *swp1* son *swp1s0*, *swp1s1*, *swp1s2* y *swp1s3*.
- El interruptor S2 se reemplaza primero por el interruptor *sw2* y luego el interruptor S1 se reemplaza por el interruptor *sw1*.
 - Luego, el cableado entre los nodos y S2 se desconecta de S2 y se vuelve a conectar a *sw2*.
 - A continuación, se desconecta el cableado entre los nodos y S1 de S1 y se vuelve a conectar a *sw1*.

Paso 1: Prepararse para la migración

1. Si AutoSupport está habilitado, suprima la creación automática de casos mediante la invocación de 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. Determinar el estado administrativo u operativo de cada interfaz de almacenamiento:

Cada puerto debería mostrarse habilitado para **Status** .

Paso 2: Configurar cables y puertos

1. Mostrar los atributos del puerto de red:

```
storage port show
```

Mostrar ejemplo

```
cluster1::*> storage port show
                                         Speed
                                         (Gb/s)
                                         VLAN
Node      Port Type  Mode      State    Status     ID
-----  -----  -----  -----  -----  -----  -----
node1
          e0c  ENET  storage  100  enabled  online   30
          e0d  ENET  storage   0  enabled  offline   30
          e5a  ENET  storage   0  enabled  offline   30
          e5b  ENET  storage  100  enabled  online   30
node2
          e0c  ENET  storage  100  enabled  online   30
          e0d  ENET  storage   0  enabled  offline   30
          e5a  ENET  storage   0  enabled  offline   30
          e5b  ENET  storage  100  enabled  online   30
cluster1::*
```

2. Verifique que los puertos de almacenamiento de cada nodo estén conectados a los commutadores de almacenamiento existentes de la siguiente manera (desde la perspectiva de los nodos) utilizando el comando:

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

Mostrar ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----  -----  -----  -----  -----
-----  -----
node1      /lldp
          e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/1      -
          e5b    S2 (7c:ad:4f:98:8e:3c)    Eth1/1      -
node2      /lldp
          e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/2      -
          e5b    S2 (7c:ad:4f:98:8e:3c)    Eth1/2      -
```

3. En los switches S1 y S2, asegúrese de que los puertos de almacenamiento y los switches estén conectados de la siguiente manera (desde la perspectiva de los switches) utilizando el comando:

```
show lldp neighbors
```

Mostrar ejemplo

```
S1# show lldp neighbors
```

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station

(O) Other

Device-ID Port ID	Local Intf	Holdtime	Capability
node1 e0c	Eth1/1	121	S
node2 e0c	Eth1/2	121	S
SHFGD1947000186 e0a	Eth1/10	120	S
SHFGD1947000186 e0a	Eth1/11	120	S
SHFGB2017000269 e0a	Eth1/12	120	S
SHFGB2017000269 e0a	Eth1/13	120	S

```
S2# show lldp neighbors
```

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station

(O) Other

Device-ID Port ID	Local Intf	Holdtime	Capability
node1 e5b	Eth1/1	121	S
node2 e5b	Eth1/2	121	S
SHFGD1947000186 e0b	Eth1/10	120	S
SHFGD1947000186 e0b	Eth1/11	120	S
SHFGB2017000269 e0b	Eth1/12	120	S
SHFGB2017000269 e0b	Eth1/13	120	S

4. En el switch sw2, apague los puertos conectados a los puertos de almacenamiento y nodos de los estantes de discos.

Mostrar ejemplo

```
cumulus@sw2:~$ net add interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

5. Traslade los puertos de almacenamiento de nodos del controlador y los estantes de discos del antiguo switch S2 al nuevo switch sw2, utilizando el cableado apropiado compatible con NVIDIA SN2100.
6. En el switch sw2, active los puertos conectados a los puertos de almacenamiento de los nodos y los estantes de discos.

Mostrar ejemplo

```
cumulus@sw2:~$ net del interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

7. Verifique que los puertos de almacenamiento de cada nodo estén conectados a los conmutadores de la siguiente manera, desde la perspectiva de los nodos:

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

Mostrar ejemplo

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

Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface      Platform
-----  -----  -----
-----  -----
node1      /lldp
          e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/1        -
          e5b    sw2 (b8:ce:f6:19:1a:7e)    swp1         -
         

node2      /lldp
          e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/2        -
          e5b    sw2 (b8:ce:f6:19:1a:7e)    swp2         -
```

8. Verifique los atributos del puerto de red:

```
storage port show
```

Mostrar ejemplo

```
cluster1::*> storage port show
                                         Speed
                                         (Gb/s)
Node      Port  Type   Mode      State    Status     VLAN
-----  -----  -----  -----  -----  -----  -----
node1
          e0c  ENET  storage  100  enabled  online   30
          e0d  ENET  storage   0  enabled  offline   30
          e5a  ENET  storage   0  enabled  offline   30
          e5b  ENET  storage  100  enabled  online   30
node2
          e0c  ENET  storage  100  enabled  online   30
          e0d  ENET  storage   0  enabled  offline   30
          e5a  ENET  storage   0  enabled  offline   30
          e5b  ENET  storage  100  enabled  online   30
cluster1::*
```

9. En el switch sw2, verifique que todos los puertos de almacenamiento de nodos estén activos:

```
net show interface
```

Mostrar ejemplo

```
cumulus@sw2:~$ net show interface

  State  Name      Spd      MTU      Mode      LLDP
Summary
-----  -----  -----  -----  -----
...
...
UP      swp1      100G    9216    Trunk/L2    node1  (e5b)
Master: bridge (UP)
UP      swp2      100G    9216    Trunk/L2    node2  (e5b)
Master: bridge (UP)
UP      swp3      100G    9216    Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge (UP)
UP      swp4      100G    9216    Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge (UP)
UP      swp5      100G    9216    Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge (UP)
UP      swp6      100G    9216    Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge (UP) )
...
...
```

10. En el switch sw1, apague los puertos conectados a los puertos de almacenamiento de los nodos y los estantes de discos.

Mostrar ejemplo

```
cumulus@sw1:~$ net add interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

11. Traslade los puertos de almacenamiento de nodos del controlador y los estantes de discos del antiguo conmutador S1 al nuevo conmutador sw1, utilizando el cableado apropiado compatible con NVIDIA SN2100.
12. En el switch sw1, active los puertos conectados a los puertos de almacenamiento de los nodos y los estantes de discos.

Mostrar ejemplo

```
cumulus@sw1:~$ net del interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

13. Verifique que los puertos de almacenamiento de cada nodo estén conectados a los commutadores de la siguiente manera, desde la perspectiva de los nodos:

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

Mostrar ejemplo

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

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			
-----	-----	-----	-----
-----	-----	-----	-----
node1	/lldp		
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp1
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1
node2	/lldp		
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp2
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2

Paso 3: Verificar la configuración

1. Verifique la configuración final:

```
storage port show
```

Cada puerto debería mostrarse habilitado para `State` y habilitó para `Status`.

Mostrar ejemplo

```
cluster1::*> storage port show
                                         Speed
                                         (Gb/s)
Node      Port Type  Mode      State    Status     VLAN
-----  -----  -----  -----  -----  -----  -----
node1
        e0c  ENET  storage  100  enabled  online   30
        e0d  ENET  storage   0  enabled  offline  30
        e5a  ENET  storage   0  enabled  offline  30
        e5b  ENET  storage  100  enabled  online   30
node2
        e0c  ENET  storage  100  enabled  online   30
        e0d  ENET  storage   0  enabled  offline  30
        e5a  ENET  storage   0  enabled  offline  30
        e5b  ENET  storage  100  enabled  online   30
cluster1::*
```

2. En el switch sw2, verifique que todos los puertos de almacenamiento de nodos estén activos:

```
net show interface
```

Mostrar ejemplo

```
cumulus@sw2:~$ net show interface

  State  Name      Spd      MTU      Mode          LLDP
Summary
-----  -----  -----  -----  -----
...
...
UP      swp1      100G    9216    Trunk/L2    node1  (e5b)
Master: bridge (UP)
UP      swp2      100G    9216    Trunk/L2    node2  (e5b)
Master: bridge (UP)
UP      swp3      100G    9216    Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge (UP)
UP      swp4      100G    9216    Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge (UP)
UP      swp5      100G    9216    Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge (UP)
UP      swp6      100G    9216    Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge (UP) )
...
...
```

3. Verifique que ambos nodos tengan una conexión a cada conmutador:

```
net show lldp
```

Mostrar ejemplo

El siguiente ejemplo muestra los resultados correspondientes para ambos interruptores:

```
cumulus@sw1:~$ net show lldp
LocalPort  Speed  Mode      RemoteHost      RemotePort
-----  -----  -----  -----
...
swp1      100G  Trunk/L2  node1          e0c
swp2      100G  Trunk/L2  node2          e0c
swp3      100G  Trunk/L2  SHFFG1826000112  e0a
swp4      100G  Trunk/L2  SHFFG1826000112  e0a
swp5      100G  Trunk/L2  SHFFG1826000102  e0a
swp6      100G  Trunk/L2  SHFFG1826000102  e0a

cumulus@sw2:~$ net show lldp
LocalPort  Speed  Mode      RemoteHost      RemotePort
-----  -----  -----  -----
...
swp1      100G  Trunk/L2  node1          e5b
swp2      100G  Trunk/L2  node2          e5b
swp3      100G  Trunk/L2  SHFFG1826000112  e0b
swp4      100G  Trunk/L2  SHFFG1826000112  e0b
swp5      100G  Trunk/L2  SHFFG1826000102  e0b
swp6      100G  Trunk/L2  SHFFG1826000102  e0b
```

4. Vuelva a cambiar el nivel de privilegios a administrador:

```
set -privilege admin
```

5. Si desactivaste la creación automática de casos, vuelve a activarla mediante un mensaje de AutoSupport :

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

¿Qué sigue?

Después de migrar tus switches, puedes ["configurar la monitorización del estado del conmutador"](#).

Reemplazar un conmutador de almacenamiento NVIDIA SN2100

Puedes reemplazar un conmutador de almacenamiento NVIDIA SN2100 defectuoso. Este es un procedimiento que no produce interrupciones.

Antes de empezar

Antes de instalar el software Cumulus y los RCF en un conmutador de almacenamiento NVIDIA SN2100, asegúrese de lo siguiente:

- Su sistema puede admitir conmutadores de almacenamiento NVIDIA SN2100.
- Has descargado los formularios RCF correspondientes.

El "Hardware Universe" Proporciona todos los detalles de los puertos compatibles y sus configuraciones.

La configuración de red existente debe tener las siguientes características:

- Completa todos los pasos de solución de problemas para confirmar que necesitas reemplazar tu interruptor.
- Asegúrese de que exista conectividad de gestión en ambos conmutadores.



Asegúrese de que se hayan completado todos los pasos de solución de problemas para confirmar que su interruptor necesita ser reemplazado.

El switch NVIDIA SN2100 de repuesto debe tener las siguientes características:

- La conectividad de la red de gestión funciona correctamente.
- Puedes acceder al interruptor de repuesto usando la consola.
- La imagen del sistema operativo RCF y Cumulus correspondiente se carga en el switch.
- La personalización inicial del switch está completa.

Resumen del procedimiento

Este procedimiento reemplaza el segundo conmutador de almacenamiento NVIDIA SN2100 sw2 con el nuevo conmutador NVIDIA SN2100 nsw2. Los dos nodos son nodo1 y nodo2.

Pasos a seguir:

- Confirme que el interruptor que se va a reemplazar es el SW2.
- Desconecta los cables del interruptor sw2.
- Vuelva a conectar los cables al interruptor nsw2.
- Verifique todas las configuraciones de los dispositivos en el switch nsw2.

Pasos

1. Si AutoSupport está habilitado en este clúster, suprime la creación automática de casos invocando un mensaje de AutoSupport :

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

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
```

3. Compruebe el estado de salud de los puertos del nodo de almacenamiento para confirmar la conexión con el conmutador de almacenamiento S1:

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

Mostrar ejemplo

```
cluster1::*> storage port show -port-type ENET
                                         Speed
                                         (Gb/s)
                                         VLAN
Node      Port Type  Mode      State    Status     ID
-----  -----  -----  -----  -----  -----  -----
node1
        e3a  ENET  storage  100  enabled  online   30
        e3b  ENET  storage   0  enabled  offline   30
        e7a  ENET  storage   0  enabled  offline   30
        e7b  ENET  storage  100  enabled  online   30
node2
        e3a  ENET  storage  100  enabled  online   30
        e3b  ENET  storage   0  enabled  offline   30
        e7a  ENET  storage   0  enabled  offline   30
        e7b  ENET  storage  100  enabled  online   30
cluster1::*
```

4. Verifique que el interruptor de almacenamiento sw1 esté disponible:

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

Mostrar ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----
node1/lldp
      e0M    sw1  (00:ea:bd:68:6a:e8)    Eth1/46      -
      e0b    sw2  (6c:b2:ae:5f:a5:b2)    Ethernet1/16  -
      e0c    SHFFG1827000286 (d0:39:ea:1c:16:92)
                  e0a          -
      e0e    sw3  (6c:b2:ae:5f:a5:ba)    Ethernet1/18  -
      e0f    SHFFG1827000286 (00:a0:98:fd:e4:a9)
                  e0b          -
      e0g    sw4  (28:ac:9e:d5:4a:9c)    Ethernet1/11  -
      e0h    sw5  (6c:b2:ae:5f:a5:ca)    Ethernet1/22  -
      e1a    sw6  (00:f6:63:10:be:7c)    Ethernet1/33  -
      e1b    sw7  (00:f6:63:10:be:7d)    Ethernet1/34  -
      e2a    sw8  (b8:ce:f6:91:3d:88)    Ethernet1/35  -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

5. Ejecutar el `net show interface` Comando en el interruptor de funcionamiento para confirmar que puede ver ambos nodos y todos los estantes:

```
net show interface
```

Mostrar ejemplo

```
cumulus@sw1:~$ net show interface

  State  Name      Spd      MTU      Mode      LLDP
Summary
-----  -----  -----  -----  -----
...
...
UP      swp1      100G    9216    Trunk/L2    node1  (e3a)
Master: bridge (UP)
UP      swp2      100G    9216    Trunk/L2    node2  (e3a)
Master: bridge (UP)
UP      swp3      100G    9216    Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge (UP)
UP      swp4      100G    9216    Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge (UP)
UP      swp5      100G    9216    Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge (UP)
UP      swp6      100G    9216    Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge (UP) )
...
...
```

6. Verifique los puertos de los estantes en el sistema de almacenamiento:

```
storage shelf port show -fields remote-device, remote-port
```

Mostrar ejemplo

```
cluster1::*> storage shelf port show -fields remote-device, remote-port
shelf    id  remote-port    remote-device
-----  --  -----  -----
3.20    0    swp3        sw1
3.20    1    -           -
3.20    2    swp4        sw1
3.20    3    -           -
3.30    0    swp5        sw1
3.20    1    -           -
3.30    2    swp6        sw1
3.20    3    -           -
cluster1::*
```

7. Retire todos los cables conectados al interruptor de almacenamiento sw2.
8. Vuelva a conectar todos los cables al interruptor de reemplazo nsw2.
9. Vuelva a comprobar el estado de salud de los puertos del nodo de almacenamiento:

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

Mostrar ejemplo

```
cluster1::*> storage port show -port-type ENET
                                         Speed
                                         (Gb/s)      VLAN
Node          Port  Type  Mode      State    Status     ID
-----  -----  -----  -----  -----  -----
node1
          e3a  ENET  storage  100  enabled  online   30
          e3b  ENET  storage   0  enabled  offline   30
          e7a  ENET  storage   0  enabled  offline   30
          e7b  ENET  storage  100  enabled  online   30
node2
          e3a  ENET  storage  100  enabled  online   30
          e3b  ENET  storage   0  enabled  offline   30
          e7a  ENET  storage   0  enabled  offline   30
          e7b  ENET  storage  100  enabled  online   30
cluster1::*
```

10. Verifique que ambos interruptores están disponibles:

```
net device-discovery show -protocol lldp
```

Mostrar ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface
Platform

-----
-----
node1/lldp
      e0M    sw1  (00:ea:bd:68:6a:e8)    Eth1/46      -
      e0b    sw2  (6c:b2:ae:5f:a5:b2)    Ethernet1/16  -
      e0c    SHFFG1827000286 (d0:39:ea:1c:16:92)
                  e0a          -
      e0e    sw3  (6c:b2:ae:5f:a5:ba)    Ethernet1/18  -
      e0f    SHFFG1827000286 (00:a0:98:fd:e4:a9)
                  e0b          -
      e0g    sw4  (28:ac:9e:d5:4a:9c)    Ethernet1/11  -
      e0h    sw5  (6c:b2:ae:5f:a5:ca)    Ethernet1/22  -
      e1a    sw6  (00:f6:63:10:be:7c)    Ethernet1/33  -
      e1b    sw7  (00:f6:63:10:be:7d)    Ethernet1/34  -
      e2a    sw8  (b8:ce:f6:91:3d:88)    Ethernet1/35  -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

11. Verifique los puertos de los estantes en el sistema de almacenamiento:

```
storage shelf port show -fields remote-device, remote-port
```

Mostrar ejemplo

```
cluster1::*> storage shelf port show -fields remote-device, remote-port
shelf    id    remote-port    remote-device
-----  --  -----
3.20     0    swp3        sw1
3.20     1    swp3        nsw2
3.20     2    swp4        sw1
3.20     3    swp4        nsw2
3.30     0    swp5        sw1
3.20     1    swp5        nsw2
3.30     2    swp6        sw1
3.20     3    swp6        nsw2
cluster1::*
```

12. Vuelva a cambiar el nivel de privilegios a administrador:

```
set -privilege admin
```

13. Si desactivaste la creación automática de casos, vuelve a activarla mediante un mensaje de AutoSupport :

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

¿Que sigue?

Después de haber reemplazado los interruptores, puedes ["configurar la monitorización del estado del conmutador"](#).

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Impreso 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.