



Switches de fin de disponibilidad

Cluster and storage switches

NetApp
April 25, 2024

Tabla de contenidos

Switches de fin de disponibilidad	1
Fin de la disponibilidad	1
Cisco Nexus 3232C	1
Cisco Nexus 3132Q-V	211
Cisco Nexus 92300YC	407
CN1610 de NetApp	530

Switches de fin de disponibilidad

Fin de la disponibilidad

Los siguientes switches ya no se pueden comprar, pero siguen siendo compatibles.

- ["Cisco Nexus 3232C"](#)
- ["Cisco Nexus 3132Q-V"](#)
- ["Cisco Nexus 92300YC"](#)
- ["CN1610 de NetApp"](#)

Cisco Nexus 3232C

Descripción general

Descripción general de la instalación y la configuración de los switches Cisco Nexus 3232c

Los switches Cisco Nexus 3232C se pueden utilizar como switches de clúster en su clúster AFF o FAS. Los switches de clúster permiten crear clústeres de ONTAP con más de dos nodos.

Información general de configuración inicial

Para configurar inicialmente un switch Cisco Nexus 3232c en sistemas que ejecutan ONTAP, siga estos pasos:

1. ["Complete la hoja de trabajo de cableado Cisco Nexus 3232C"](#). La hoja de cálculo de cableado de ejemplo proporciona ejemplos de asignaciones de puertos recomendadas desde los switches a las controladoras. La hoja de datos en blanco proporciona una plantilla que puede utilizar para configurar su clúster.
2. ["Instale un switch de clúster Cisco Nexus 3232C en un armario de NetApp"](#). Instale el switch de clúster Cisco Nexus 3232C y el panel de paso a través de un armario de NetApp con los soportes estándar que se incluyen con el switch.
3. ["Configure el switch del clúster 3232C"](#). Configure y configure el switch Cisco Nexus 3232C.
4. ["Prepare la instalación del software NX-OS y del archivo de configuración de referencia"](#). Prepare la instalación del software NX-OS y del archivo de configuración de referencia (RCF).
5. ["Instale el software NX-OS"](#). Instale el software NX-OS en el switch de clúster Nexus 3232C.
6. ["Instalación del archivo de configuración de referencia \(RCF\)"](#). Instale el RCF después de configurar el interruptor Nexus 3232C por primera vez. También puede utilizar este procedimiento para actualizar la versión de RCF.

Información adicional

Antes de iniciar la instalación o el mantenimiento, asegúrese de revisar lo siguiente:

- ["Requisitos de configuración"](#)
- ["Documentación requerida"](#)

- ["Requisitos de Smart Call Home"](#)

Requisitos de configuración de los switches Cisco Nexus 3232C

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

Requisitos de configuración

Para configurar el clúster, necesita el número y el tipo de cables y conectores de cable adecuados para los switches. Según el tipo de switch que esté configurando inicialmente, debe conectarse al puerto de la consola del switch con el cable de consola incluido; también debe proporcionar información de red específica.

Requisitos de red

Necesita la siguiente información de red para todas las configuraciones de los switches:

- Subred IP para el tráfico de red de gestión
- Nombres de host y direcciones IP para cada una de las controladoras del sistema de almacenamiento y todos los switches aplicables
- La mayoría de las controladoras del sistema de almacenamiento se gestionan a través de la interfaz e0M mediante la conexión al puerto de servicio Ethernet (icono de llave inglesa). En los sistemas A800 y A700 de AFF de AFF, la interfaz e0M utiliza un puerto Ethernet dedicado.

Consulte la ["Hardware Universe"](#) para obtener la información más reciente.

Requisitos de documentación para los switches Cisco Nexus 3232C

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

Documentación de los switches

Para configurar los switches Cisco Nexus 3232C, necesita la siguiente documentación de ["Compatibilidad con los 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 acerca de los requisitos del sitio, detalles del switch de hardware y las opciones de instalación.
<i>Guías de configuración del software del switch Cisco Nexus serie 3000</i> (elija la guía para la versión NX-OS instalada en los switches)	Proporciona la información inicial de configuración del switch que necesita para poder configurar el switch para el funcionamiento de ONTAP.

Título del documento	Descripción
<i>Guía de actualización y degradación de software NX-OS de Cisco Nexus 3000 Series</i> (elija la guía para la versión de NX-OS instalada en los switches)	Proporciona información sobre cómo degradar el switch a software de switch compatible con ONTAP, si es necesario.
<i>Cisco Nexus 3000 Series NX-OS Command Reference Master Index</i>	Proporciona vínculos a las diferentes referencias de comandos proporcionadas por Cisco.
<i>Cisco Nexus 3000 MIBs Reference</i>	Describe los archivos de la base de datos de información de gestión (MIB) para los switches Nexus 3000.
<i>Referencia de mensajes del sistema NX-OS serie Nexus 3000</i>	Describe los mensajes del sistema de los switches Cisco Nexus serie 3000, los 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 Cisco Nexus serie 3000 NX-OS (elija las notas para la versión de NX-OS instalada en los switches)</i>	Describe las funciones, errores y limitaciones de Cisco Nexus 3000 Series.
Información sobre cumplimiento de normativas y seguridad de Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series y Cisco Nexus 2000 Series	Proporciona información legal, de seguridad y cumplimiento de normativas de agencias 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 desde la ["Centro de documentación de ONTAP 9"](#).

Nombre	Descripción
Específicos del controlador <i>instrucciones de instalación y configuración</i>	Describe cómo instalar el hardware de NetApp.
Documentación de ONTAP	Proporciona información detallada sobre todos los aspectos de las versiones de ONTAP.
"Hardware Universe"	Ofrece información de compatibilidad y configuración de hardware de NetApp.

Kit de raíl y documentación del armario

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

Nombre	Descripción
"Armario del sistema 42U, guía detallada"	Describe las FRU asociadas al armario del sistema 42U, y proporciona instrucciones de mantenimiento y sustitución de FRU.
"Instale un switch Cisco Nexus 3232C en un armario de NetApp"	Describe cómo instalar un switch Cisco Nexus 3232C en un armario de cuatro parantes de NetApp.

Requisitos de Smart Call Home

Para utilizar la función de inicio de llamada inteligente, revise las siguientes directrices.

Smart Call Home supervisa los componentes de hardware y software de su red. Cuando se produce una configuración de sistema crítica, genera una notificación basada en correo electrónico y genera una alerta a todos los destinatarios que están configurados en el perfil de destino. 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 el conmutador de red de clúster para aprovechar la función integrada de soporte Smart Call Home de Cisco.

Antes de poder utilizar Smart Call Home, tenga en cuenta las siguientes consideraciones:

- Debe haber un servidor de correo electrónico.
- El switch debe tener conectividad IP con el servidor de correo electrónico.
- Se debe configurar el nombre del contacto (contacto del servidor SNMP), el número de teléfono y la dirección de la calle. Esto es necesario para determinar el origen de los mensajes recibidos.
- Un ID de CCO debe estar asociado con un contrato de servicio Cisco SMARTnet adecuado para su empresa.
- El servicio Cisco SMARTnet debe estar en su lugar para que el dispositivo se registre.

La ["Sitio de soporte de Cisco"](#) Contiene información acerca de los comandos para configurar Smart Call Home.

Instale el hardware

Complete la hoja de trabajo de cableado Cisco Nexus 3232C

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

La hoja de cálculo de cableado de ejemplo proporciona ejemplos de asignaciones de puertos recomendadas desde los switches a las controladoras. La hoja de datos en blanco proporciona una plantilla que puede utilizar para configurar su clúster.

Cada switch puede configurarse como un único puerto de 100 GbE, 40 GbE o 4 puertos de 10 GbE.

Hoja de trabajo para el cableado de muestra

La definición de puerto de ejemplo de cada par de conmutadores es la siguiente:

Switch de clúster a		Switch del clúster B	
Puerto del switch	Uso de nodos y puertos	Puerto del switch	Uso de nodos y puertos
1	4 x 10 GbE/4 GbE o nodo 40/100GbE	1	4 x 10 GbE/4 GbE o nodo 40/100GbE
2	4 x 10 GbE/4 GbE o nodo 40/100GbE	2	4 x 10 GbE/4 GbE o nodo 40/100GbE
3	4 x 10 GbE/4 GbE o nodo 40/100GbE	3	4 x 10 GbE/4 GbE o nodo 40/100GbE
4	4 x 10 GbE/4 GbE o nodo 40/100GbE	4	4 x 10 GbE/4 GbE o nodo 40/100GbE
5	4 x 10 GbE/4 GbE o nodo 40/100GbE	5	4 x 10 GbE/4 GbE o nodo 40/100GbE
6	4 x 10 GbE/4 GbE o nodo 40/100GbE	6	4 x 10 GbE/4 GbE o nodo 40/100GbE
7	4 x 10 GbE/4 GbE o nodo 40/100GbE	7	4 x 10 GbE/4 GbE o nodo 40/100GbE
8	4 x 10 GbE/4 GbE o nodo 40/100GbE	8	4 x 10 GbE/4 GbE o nodo 40/100GbE
9	4 x 10 GbE/4 GbE o nodo 40/100GbE	9	4 x 10 GbE/4 GbE o nodo 40/100GbE
10	4 x 10 GbE/4 GbE o nodo 40/100GbE	10	4 x 10 GbE/4 GbE o nodo 40/100GbE
11	4 x 10 GbE/4 GbE o nodo 40/100GbE	11	4 x 10 GbE/4 GbE o nodo 40/100GbE
12	4 x 10 GbE/4 GbE o nodo 40/100GbE	12	4 x 10 GbE/4 GbE o nodo 40/100GbE
13	4 x 10 GbE/4 GbE o nodo 40/100GbE	13	4 x 10 GbE/4 GbE o nodo 40/100GbE
14	4 x 10 GbE/4 GbE o nodo 40/100GbE	14	4 x 10 GbE/4 GbE o nodo 40/100GbE

Switch de clúster a		Switch del clúster B	
15	4 x 10 GbE/4 GbE o nodo 40/100GbE	15	4 x 10 GbE/4 GbE o nodo 40/100GbE
16	4 x 10 GbE/4 GbE o nodo 40/100GbE	16	4 x 10 GbE/4 GbE o nodo 40/100GbE
17	4 x 10 GbE/4 GbE o nodo 40/100GbE	17	4 x 10 GbE/4 GbE o nodo 40/100GbE
18	4 x 10 GbE/4 GbE o nodo 40/100GbE	18	4 x 10 GbE/4 GbE o nodo 40/100GbE
19	19 nodos 40g/100GbE	19	19 nodos 40g/100GbE
20	20 nodos 40g/100GbE	20	20 nodos 40g/100GbE
21	21 nodos 40g/100GbE	21	21 nodos 40g/100GbE
22	22 nodos 40g/100GbE	22	22 nodos 40g/100GbE
23	23 nodos 40g/100GbE	23	23 nodos 40g/100GbE
24	24 nodos 40g/100GbE	24	24 nodos 40g/100GbE
25 hasta 30	Reservado	25 hasta 30	Reservado
31	100GbE ISL al puerto 31 del switch B	31	100GbE ISL para conmutar Un puerto 31
32	100GbE ISL al puerto 32 del switch B	32	100GbE ISL para conmutar Un puerto 32

Hoja de trabajo de cableado en blanco

Puede utilizar la hoja de datos de cableado vacía para documentar las plataformas que se admiten como nodos de un clúster. La sección *Cluster Connections* del "[Hardware Universe](#)" define los puertos de clúster que utiliza la plataforma.

Switch de clúster a		Switch del clúster B	
Puerto del switch	Uso del nodo/puerto	Puerto del switch	Uso del nodo/puerto
1		1	
2		2	

Switch de clúster a		Switch del clúster B	
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	
20		20	
21		21	
22		22	
23		23	
24		24	

Switch de clúster a		Switch del clúster B	
25 hasta 30	Reservado	25 hasta 30	Reservado
31	100GbE ISL al puerto 31 del switch B	31	100GbE ISL para conmutar Un puerto 31
32	100GbE ISL al puerto 32 del switch B	32	100GbE ISL para conmutar Un puerto 32

Configure el switch del clúster 3232C

Siga este procedimiento para configurar el switch Cisco Nexus 3232C.

Lo que necesitará

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones correspondientes del NX-OS y del archivo de configuración de referencia (RCF).
- La versión aplicable de NX-OS, descargada del ["Descarga de software de Cisco"](#) página.
- Documentación necesaria sobre la red de clúster y el switch de red de gestión.

Consulte ["Documentación requerida"](#) si quiere más información.

- Documentación requerida de la controladora y documentación de ONTAP

["Documentación de NetApp"](#)

- Las licencias aplicables, la información de configuración y red, y los cables.
- Hojas de datos de cableado completadas.
- Archivos RCF de red de gestión y red de clúster de NetApp aplicables, descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#) para los switches que reciba. Todos los switches de red de gestión y red de clúster de Cisco llegan con la configuración predeterminada de fábrica de Cisco. Estos conmutadores también tienen la versión actual del software NX-OS, pero no tienen cargados los RCF.

Pasos

1. Monte en rack la red del clúster y los switches de red de gestión y las controladoras.



Si está instalando el...	Realice lo siguiente...
Cisco Nexus 3232C en un armario del sistema de NetApp	Consulte el <i>instalación de un switch de clúster Cisco Nexus 3232C y el panel de paso a través de una guía del armario de NetApp</i> para obtener instrucciones sobre cómo instalar el switch en un armario de NetApp.
Equipo en un bastidor de Telco	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 cables de la red de clústeres y los switches de red de gestión a las controladoras mediante las hojas de trabajo de cableado completadas.

3. Encienda la red de clúster y los switches de red de gestión y las controladoras.
4. Realice una configuración inicial de los switches de red de clúster.

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

Prompt	Respuesta
¿Desea anular el aprovisionamiento automático y continuar con la configuración normal? (sí/no)	Responda con sí . El valor predeterminado es no
¿Desea aplicar un estándar de contraseña segura? (sí/no)	Responda con sí . El valor predeterminado es yes.
Introduzca la contraseña para el administrador.	La contraseña predeterminada es "admin"; debe crear una nueva contraseña segura. Se puede rechazar una contraseña débil.
¿Desea introducir el cuadro de diálogo de configuración básica? (sí/no)	Responda con sí en la configuración inicial del interruptor.
¿Crear otra cuenta de inicio de sesión? (sí/no)	Su respuesta depende de las políticas de su sitio con respecto a los administradores alternativos. El valor predeterminado es no .
¿Configurar cadena de comunidad SNMP de solo lectura? (sí/no)	Responda con no . El valor predeterminado es no
¿Configurar cadena de comunidad SNMP de lectura y escritura? (sí/no)	Responda con no . El valor predeterminado es no
Introduzca el nombre del switch.	El nombre del conmutador está limitado a 63 caracteres alfanuméricos.
¿Continuar con la configuración de administración fuera de banda (mgmt0)? (sí/no)	Responda con sí (el valor predeterminado) en ese indicador. En el símbolo de sistema mgmt0 IPv4 address:, introduzca su dirección IP: ip_address.
¿Configurar la puerta de enlace predeterminada? (sí/no)	Responda con sí . En la dirección IPv4 de la solicitud default-Gateway:, introduzca su default_Gateway.
¿Configurar las opciones avanzadas de IP? (sí/no)	Responda con no . El valor predeterminado es no

Prompt	Respuesta
¿Habilitar el servicio telnet? (sí/no)	Responda con no . El valor predeterminado es no
¿Servicio SSH habilitado? (sí/no)	<p>Responda con sí. El valor predeterminado es yes.</p> <div>  <p>Se recomienda SSH cuando se utilice el Monitor de estado del conmutador de clúster (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.</p> </div>
Introduzca el tipo de clave SSH que desea generar (dsa/rsa/rsa1).	El valor predeterminado es rsa .
Introduzca el número de bits de clave (1024-2048).	Introduzca el número de bits de clave de 1024-2048.
¿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 (cerrada/nohut):	Responda con nohut . El valor predeterminado es nohut.
Configurar el perfil del sistema COPP (estricto/moderado/indulgente/denso):	Responda con estricto . El valor predeterminado es estricto.
¿Desea editar la configuración? (sí/no)	Debería ver la nueva configuración en este momento. Revise y realice los cambios necesarios en la configuración que acaba de introducir. Si está satisfecho con la configuración, responda no en el indicador. Responda con sí si desea editar los ajustes de configuración.
¿Utilizar esta configuración y guardarla? (sí/no)	<p>Responda con sí para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.</p> <div>  <p>Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador.</p> </div>

- Compruebe las opciones de configuración que ha realizado en la pantalla que aparece al final de la instalación y asegúrese de guardar la configuración.

6. Compruebe la versión de los switches de red del clúster y, si es necesario, descargue la versión del software compatible con NetApp en los switches de la "[Descarga de software de Cisco](#)" página.

El futuro

["Prepare la instalación de NX-OS y RCF"](#).

Instale un switch de clúster Cisco Nexus 3232C en un armario de NetApp

En función de la configuración, quizás necesite instalar el switch del clúster Cisco Nexus 3232C y el panel de paso a través de una cabina de NetApp con los soportes estándar que se incluyen con el switch.

Lo que necesitará

- Los requisitos iniciales de preparación, el contenido del kit y las precauciones de seguridad del "[Guía de instalación de hardware de Cisco Nexus serie 3000](#)".
- Para cada interruptor, los ocho tornillos 10-32 ó 12-24 y las tuercas de pinza para montar los soportes y rieles deslizantes en los postes del armario delantero y trasero.
- Kit de guías estándar de Cisco para instalar el switch en un armario de NetApp.



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

Pasos

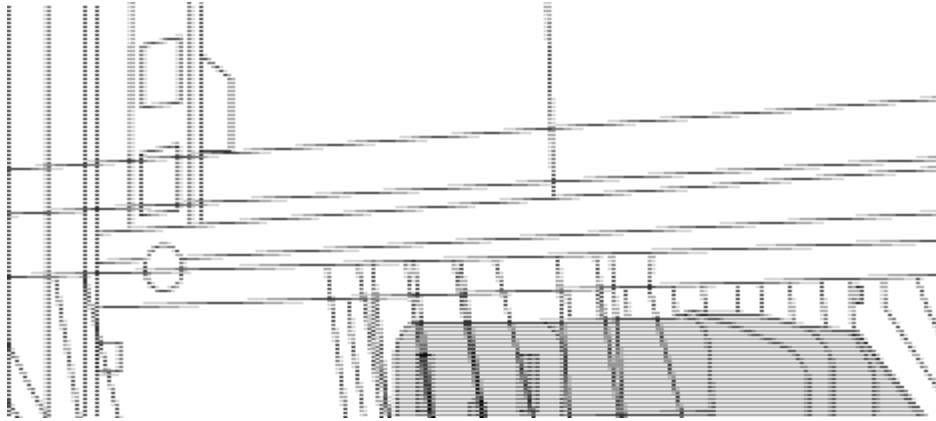
1. Instale el panel de borrado de paso en el armario de NetApp.

NetApp puede adquirir el kit de panel de paso a través (número de pieza X8784-R6).

El kit del panel de paso a través de NetApp contiene el siguiente hardware:

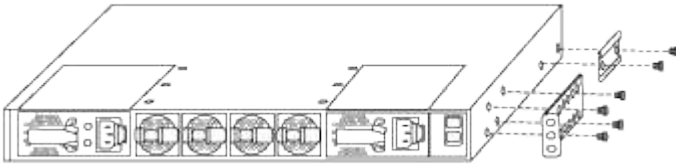
- Un panel de supresión de paso a través
- Cuatro tornillos de 10-32 x 0,75
- Cuatro tuercas de 10-32 abrazaderas
 - i. Determine la ubicación vertical de los interruptores y el panel de supresión en el armario.

En este procedimiento, el panel de limpieza se instalará en U40.
 - ii. Instale dos tuercas de abrazadera a cada lado en los orificios cuadrados adecuados para los rieles delanteros del armario.
 - iii. Centre el panel verticalmente para evitar intrusiones en el espacio adyacente del bastidor y, a continuación, 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 del cepillo.

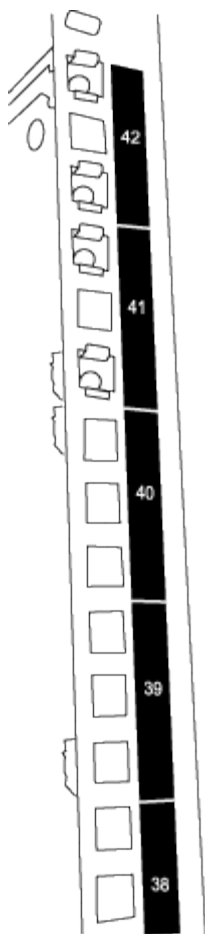


(1) *conector hembra del cable puente.*

1. Instale los soportes de montaje en rack en el chasis del switch Nexus 3232C.
 - a. Coloque un soporte de montaje de rack frontal en un lado del chasis del switch de modo que el oído de montaje esté alineado con la placa frontal del chasis (en el lado de la fuente de alimentación o del ventilador) y, a continuación, utilice cuatro tornillos M4 para conectar el soporte al chasis.



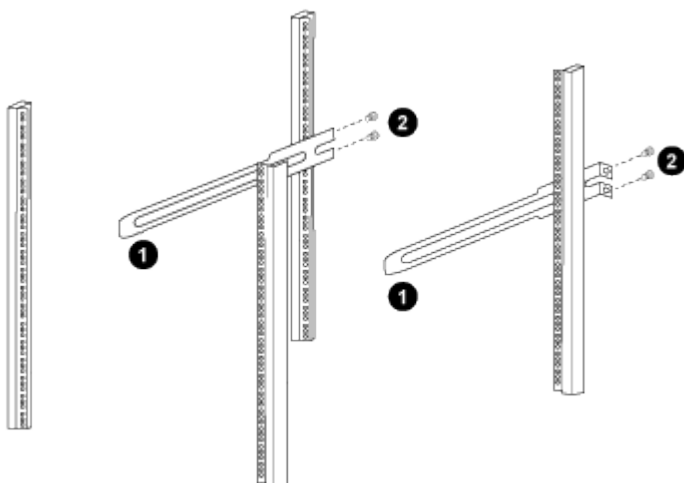
- b. Repita el paso 2a con el otro soporte de montaje en bastidor delantero en el otro lado del interruptor.
 - c. Instale el soporte de montaje en bastidor trasero en el chasis del interruptor.
 - d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del interruptor.
2. Instale las tuercas de abrazadera en las ubicaciones de los orificios cuadrados de los cuatro postes de IEA.



Los dos conmutadores 3232C siempre se montarán en el 2U superior del armario RU41 y 42.

3. Instale los rieles deslizantes en el armario.

- 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, a continuación, apriete los tornillos con los dedos.



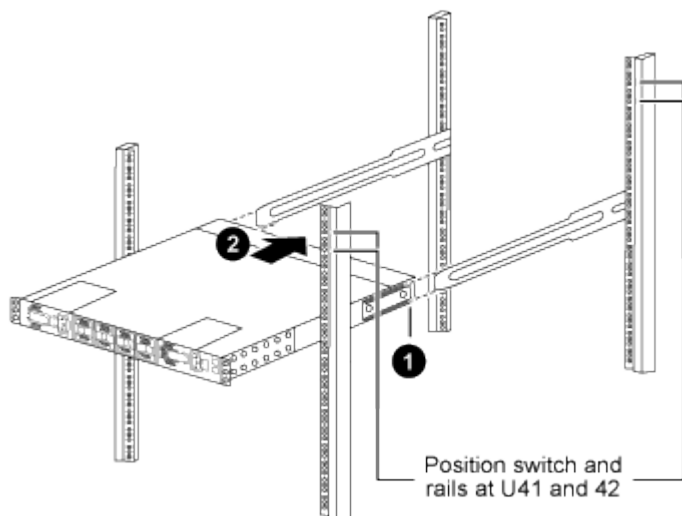
(1) mientras desliza suavemente el riel deslizante, alinéelo con los orificios de los tornillos del rack. + (2) apriete los tornillos de los rieles deslizantes a los postes del armario.

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



Este paso requiere dos personas: Una persona para sostener el interruptor desde la parte frontal y otra para guiar el interruptor hacia los rieles deslizantes traseros.

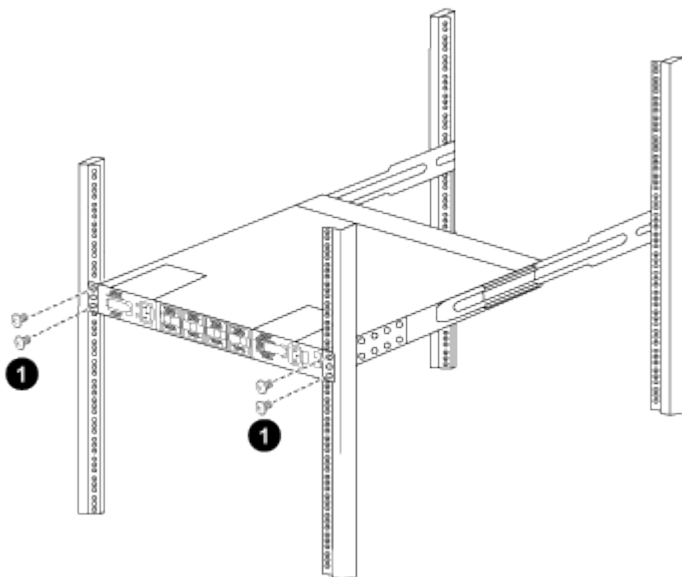
- a. Coloque la parte posterior del interruptor en RU41.



(1) a medida que el chasis se empuja hacia los postes traseros, alinee las dos guías de montaje en bastidor trasero con los rieles deslizantes.

(2) deslice suavemente el interruptor hasta que los soportes de montaje del bastidor delantero estén a ras con los postes delanteros.

- b. Conecte el interruptor al armario.



(1) con una persona sujetando la parte delantera del chasis, la otra persona debe apretar completamente los cuatro tornillos traseros a los postes del armario.

- a. Con el chasis apoyado ahora 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 mantener la parte delantera del segundo interruptor durante el proceso de instalación.

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



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

7. Conecte el puerto de gestión de cada switch 3232C a cualquiera de los switches de gestión (si se le solicita) o conéctelos directamente a su red de gestión.

El puerto de gestión es el puerto superior derecho ubicado en el lado PSU del switch. El cable CAT6 para cada switch debe enrutarse a través del panel de paso a través después de instalar los switches para conectarse a los switches de administración o a la red de gestión.

Revise las consideraciones sobre el cableado y la configuración

Antes de configurar el switch Cisco 3232C, revise las siguientes consideraciones.

Compatibilidad con los puertos NVIDIA CX6, CX6-DX y Ethernet de CX7 Gb

Si se conecta un puerto de switch a un controlador ONTAP mediante los puertos NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) o ConnectX-7 (CX7), debe codificar de forma fija la velocidad del puerto del switch.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Consulte "[Hardware Universe](#)" para obtener más información sobre los puertos de switch.

Configurar el software

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

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

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan dos nodos. Estos nodos utilizan dos puertos de interconexión de clúster de 10 GbE e0a y.. e0b.

Consulte "[Hardware Universe](#)" para verificar los puertos de clúster correctos en sus plataformas.



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

Nomenclatura de switch y nodo

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

- Los nombres de los dos switches Cisco son `cs1` y.. `cs2`.
- Los nombres de nodo son `cluster1-01` y.. `cluster1-02`.
- Los nombres de 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`.
- La `cluster1::*>` prompt indica el nombre del clúster.

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Pasos

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

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



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

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

```
set -privilege advanced
```

El aviso avanzado (***>**) aparece.

3. Muestre cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster:

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

Muestra el ejemplo

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

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

a. Mostrar los atributos del puerto de red:

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

Muestra el ejemplo

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

```
Node: cluster1-02
```

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

```
Node: cluster1-01
```

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

```
4 entries were displayed.
```

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

Muestra el ejemplo

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

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

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

4 entries were displayed.

5. Haga ping en las LIF de clúster remoto: `cluster ping-cluster -node node-name`

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node cluster1-02
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01      e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01      e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02      e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02      e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

6. Compruebe que el auto-revert El comando está habilitado en todos los LIF de clúster: `network interface show -vserver Cluster -fields auto-revert`

Muestra el ejemplo

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

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

4 entries were displayed.

7. Para ONTAP 9.8 y versiones posteriores, habilite la función de recogida de registros de control de estado del switch Ethernet para recopilar archivos de registro relacionados con el switch, mediante los comandos:

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

```
system switch ethernet log enable-collection
```

Muestra el ejemplo

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

8. Para las versiones 9.5P16, 9.6P12 y 9.7P10 de ONTAP y versiones posteriores de parches, habilite la función de recopilación de registros del monitor de estado del switch Ethernet para recopilar archivos de registro relacionados con el switch mediante los comandos: `system cluster-switch log setup-`

password

system cluster-switch log enable-collection

Muestra el ejemplo

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

Instale el software NX-OS

Puede utilizar este procedimiento para instalar el software NX-OS en el switch de clúster Nexus 3232C.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- ["Página del switch Cisco Ethernet"](#). Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.
- ["Switches Cisco Nexus serie 3000"](#). Consulte las guías de software y actualización adecuadas disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de switches de Cisco.

Instale el software

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Asegúrese de completar el procedimiento en ["Prepare la instalación de NX-OS y RCF"](#) y, a continuación, siga los pasos que se indican a continuación.

Pasos

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

Muestra el ejemplo

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

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

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

3. Copie las imágenes del software NX-OS y EPLD en el switch Nexus 3232C.

Muestra el 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.
```

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

```
show version
```

Muestra el ejemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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

Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FO?????GD

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

Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
```

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

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

5. Instale la imagen NX-OS.

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

Muestra el ejemplo

```
cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

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

Verifying image type.
[] 100% -- SUCCESS

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

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

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

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

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

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

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

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[] 100% -- SUCCESS
```

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

```
cs2#
```

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

Muestra el ejemplo

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

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

Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FO?????GD

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

  Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
```


Reason: Reset due to upgrade

System version: 9.3(3)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

cs2#

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

Muestra el 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#
```

8. Tras reiniciar el switch, vuelva a iniciar sesión, actualice la imagen dorada de EPLD y reinicie el switch una vez más.

Muestra el ejemplo

```
cs2# install epld bootflash:n9000-epld.9.3.4.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module          Type          Upgradable          Impact          Reason
-----
1              SUP              Yes              disruptive      Module
Upgradable

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

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

9. Tras reiniciar el conmutador, inicie sesión para verificar que la nueva versión de EPLD se ha cargado correctamente.

Muestra el ejemplo

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

EPLD	Device	Version
MI	FPGA	0x12
IO	FPGA	0x12

El futuro

["Instale el archivo de configuración RCF"](#)

Instalación del archivo de configuración de referencia (RCF)

Siga este procedimiento para instalar el RCF después de configurar el interruptor Nexus 3232C por primera vez.

También puede utilizar este procedimiento para actualizar la versión de RCF. Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) Para obtener más información al actualizar el RCF.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El archivo de configuración de referencia actual (RCF).
- Una conexión de consola al conmutador, necesaria para instalar el RCF.
- ["Página del switch Cisco Ethernet"](#) Consulte la tabla de compatibilidad del conmutador para conocer las versiones ONTAP y RCF admitidas. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis del comando en el RCF y la que se encuentra en las versiones de NX-OS.
- ["Switches Cisco Nexus serie 3000"](#). Consulte las guías de software y actualización adecuadas disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de switches de Cisco.

Instale el archivo

Acerca de los ejemplos

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

- Los nombres de los dos switches Cisco son cs1 y.. cs2.
- Los nombres de nodo son cluster1-01, cluster1-02, cluster1-03, y. cluster1-04.
- Los nombres de 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.

- La `cluster1::*>` prompt indica el nombre del clúster.

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Durante este procedimiento no se necesita ningún enlace entre switches (ISL) operativo. Esto se debe a que los cambios en la versión de RCF pueden afectar temporalmente a la conectividad ISL. Para garantizar operaciones de clúster no disruptivas, el siguiente procedimiento migra todas las LIF del clúster al switch de partner operativo mientras realiza los pasos del switch de destino.

Asegúrese de completar el procedimiento en "[Prepare la instalación de NX-OS y RCF](#)" y, a continuación, siga los pasos que se indican a continuación.

Pasos

1. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                Ethernet1/7      N3K-
C3232C
          e0d    cs2                Ethernet1/7      N3K-
C3232C
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N3K-
C3232C
          e0d    cs2                Ethernet1/8      N3K-
C3232C
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N3K-
C3232C
          e0b    cs2                Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N3K-
C3232C
          e0b    cs2                Ethernet1/1/2    N3K-
C3232C
cluster1::*>
```

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

a. Compruebe que todos los puertos del clúster tengan el estado correcto:

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

Muestra el 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

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

cluster1::*>

b. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

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


Muestra el ejemplo

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	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. Compruebe que el clúster muestra información de ambos switches de clúster:

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

Muestra el ejemplo

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

Switch Model	Type	Address
cs1 NX3232C	cluster-network	10.233.205.92
Serial Number: FOXXXXXXXXGS		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
9.3(4)		
Version Source: CDP		
cs2 NX3232C	cluster-network	10.233.205.93
Serial Number: FOXXXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
9.3(4)		
Version Source: CDP		

2 entries were displayed.

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

Muestra el ejemplo

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

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

Muestra el ejemplo

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

5. Comprobar que los puertos del clúster han migrado a los puertos alojados en el switch cs1 del clúster. Esto puede tardar unos segundos.

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

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

6. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el 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::*>
```

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

```
show running-config
```

8. Limpie la configuración del interruptor CS2 y reinicie el interruptor.



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

- a. Limpie la configuración:

Muestra el ejemplo

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Reinicie el switch:

Muestra el ejemplo

```
(cs2)# reload

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

9. Realice una configuración básica del interruptor. Consulte ["Configure el switch del clúster 3232C"](#) para obtener más detalles.

10. Copie el RCF en el bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

Muestra el ejemplo

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

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

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

Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

Muestra el ejemplo

En este ejemplo se muestra el archivo RCF Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt instalación en el conmutador cs2:

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

12. Examine el resultado del banner desde el `show banner motd` comando. Debe leer y seguir las instrucciones que se indican en **Notas importantes** para asegurarse de que la configuración y el funcionamiento del interruptor son correctos.

Muestra el ejemplo

```
cs2# show banner motd
```

```
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Cisco Nexus 3232C
* Filename    : Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date       : Oct-20-2020
* Version    : v1.6
*
* Port Usage : Breakout configuration
* Ports 1- 3: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25GbE) Intra-Cluster/HA Ports, int
e1/4/1-4,
* e1/5/1-4, e1/6/1-4
* Ports 7-30: 40/100GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
* Ports 33-34: 10GbE Intra-Cluster 10GbE Ports, int e1/33-34
*
* IMPORTANT NOTES
* - Load Nexus_3232C_RCF_v1.6-Cluster-HA.txt for non breakout config
*
* - This RCF utilizes QoS and requires TCAM re-configuration,
requiring RCF
*   to be loaded twice with the Cluster Switch rebooted in between.
*
* - Perform the following 4 steps to ensure proper RCF installation:
*
*   (1) Apply RCF first time, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class IPv4
ingress...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*       - Syntax error while parsing...
```

```
*
* (4) Save running-configuration again
*****
*****
```



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

13. Compruebe que el archivo RCF es la versión más reciente correcta:

```
show running-config
```

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

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

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

14. Después de comprobar que las versiones de RCF y los ajustes del switch son correctos, copie el archivo running-config en el archivo startup-config.

Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

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

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

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

16. Aplique el mismo RCF y guarde la configuración en ejecución por segunda vez.

Muestra el ejemplo

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands  
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

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

a. Compruebe que los puertos e0d están en buen estado y en todos los nodos del clúster:

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


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

Muestra el ejemplo

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

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			
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: FOXXXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
9.3(4)		
Version Source: CDP		
cs2	cluster-network	10.233.205.91

```
N3K-C3232C
  Serial Number: FOXXXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                9.3(4)
  Version Source: CDP

2 entries were displayed.
```

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



```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-
BLOCK_PVID_PEER: Blocking port-channel1 on VLAN0001.
Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-
BLOCK_PVID_LOCAL: Blocking port-channel1 on VLAN0092.
Inconsistent local vlan.
```



Los nodos del clúster pueden tardar hasta 5 minutos en informar en buen estado.

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

Muestra el ejemplo

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

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

19. Comprobar que las LIF del clúster han migrado a los puertos alojados en el switch cs2. Esto puede tardar unos segundos.

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

Muestra el 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	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	false		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		
8 entries were displayed.				
cluster1::*>				

20. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el 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::*>
```

21. Repita los pasos 7 a 15 en el interruptor CS1.
22. Habilite la reversión automática en las LIF del clúster.

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

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

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

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

Muestra el 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)  --
.
.
```

25. Compruebe que el ISL entre cs1 y cs2 funciona:

```
show port-channel summary
```

Muestra el ejemplo

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
      Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
cs1#
```

26. Compruebe que las LIF del clúster han vuelto a su puerto de inicio:

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

Muestra el 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 de las LIF de clúster no ha vuelto a sus puertos raíz, revierte manualmente: `network interface revert -vserver vservice_name -lif lif_name`

27. Compruebe que el clúster esté en buen estado:

```
cluster show
```


Muestra el 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::*>
```

28. Haga ping en las interfaces de clúster remoto para verificar la conectividad:

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Recopilación de registro de supervisión del estado del switch Ethernet

Es posible usar la función de recopilación de registros para recoger archivos de registro relacionados con switches en ONTAP. El monitor de estado del switch Ethernet (CSHM)

es responsable de garantizar el estado operativo de los conmutadores de red del clúster y de almacenamiento y de recopilar registros del switch para fines de depuración. Este procedimiento lo guía a través del proceso de configuración e inicio de la recopilación de registros detallados de **Soporte** desde el switch e inicia una recopilación por hora de datos **Periódicos** que es recopilada por AutoSupport.

Antes de empezar

- Compruebe que ha configurado su entorno mediante el conmutador de clúster de Cisco 3232C **CLI**.
- La monitorización del estado del interruptor debe estar activada para el interruptor. Verifique esto asegurándose de que el `Is Monitored`: el campo se establece en **true** en la salida del `system switch ethernet show` comando.

Pasos

1. Cree una contraseña para la función de recogida de registros de monitor de estado del switch Ethernet:

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

Muestra el ejemplo

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

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

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

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

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

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

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

2. Para iniciar la recopilación de registros, ejecute el siguiente comando, sustituyendo EL DISPOSITIVO por el conmutador utilizado en el comando anterior. Esto inicia ambos tipos de recopilación de registros: Los

registros detallados de **Support** y una recopilación horaria de datos **Periódicos**.

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

Muestra el ejemplo

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.


cluster1::*> system switch ethernet log modify -device cs2 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.
```

Espere 10 minutos y compruebe que se complete la recopilación de registros:

```
system switch ethernet log show
```



Si alguno de estos comandos devuelve un error o si la recogida de registros no se completa, póngase en contacto con el soporte de NetApp.

Resolución de problemas

Si se encuentra con alguno de los siguientes estados de error informados por la función de recopilación de registros (visible en la salida de `system switch ethernet log show`), pruebe los pasos de depuración correspondientes:

Estado de error de recopilación de registros	Resolución
Las claves RSA no están presentes	Vuelva a generar las claves SSH de ONTAP. Póngase en contacto con el soporte de NetApp.
error de contraseña de cambio	Verifique las credenciales, pruebe la conectividad SSH y vuelva a generar las claves SSH de ONTAP. Revise la documentación del switch o póngase en contacto con el soporte de NetApp para obtener instrucciones.

Las claves ECDSA no están presentes para FIPS	Si el modo FIPS está activado, es necesario generar claves ECDSA en el conmutador antes de volver a intentarlo.
registro preexistente encontrado	Elimine el archivo de recopilación de registros anterior del conmutador.
error de registro de volcado del interruptor	Asegúrese de que el usuario del conmutador tiene permisos de recopilación de registros. Consulte los requisitos previos anteriores.

Configurar SNMPv3

Siga este procedimiento para configurar SNMPv3, que admite la monitorización del estado del switch Ethernet (CSHM).

Acerca de esta tarea

Los siguientes comandos configuran un nombre de usuario SNMPv3 en switches Cisco 3232C:

- Para **sin autenticación**: `snmp-server user SNMPv3_USER NoAuth`
- Para **autenticación MD5/SHA**: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- Para autenticación **MD5/SHA con cifrado AES/DES**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication-method usm -remote-switch-ipaddress ADDRESS`

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

Pasos

1. Configure el usuario SNMPv3 en el conmutador para que utilice autenticación y cifrado:

```
show snmp user
```

Muestra el ejemplo

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1) (Config)# show snmp user

-----
-----
                                SNMP USERS
-----
-----

User              Auth              Priv(enforce)    Groups
acl_filter
-----
-----
admin             md5              des(no)          network-admin
SNMPv3User        md5              aes-128(no)      network-operator
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

User              Auth              Priv
-----
-----

(sw1) (Config)#
```

2. Configure el usuario SNMPv3 en el lado ONTAP:

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

Muestra el ejemplo

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configure CSHM para monitorizar con el nuevo usuario de SNMPv3:

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

Muestra el ejemplo

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

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N3K-C3232C
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

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

4. Compruebe que el número de serie que se va a consultar con el usuario SNMPv3 recién creado es el mismo que se detalla en el paso anterior después de que se haya completado el período de sondeo de CSHM.

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


Muestra el ejemplo

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

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

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N3K-C3232C
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Migrar switches

Requisitos de migración para los switches de clúster Cisco Nexus 3232C

Antes de migrar a switches de clúster Cisco Nexus 3232C, revise la información de configuración, las conexiones de puertos y los requisitos de cableado.

Requisitos de migración de CN1610

Los switches de clúster admiten las siguientes conexiones de nodo:

- NetApp CN1610: Puertos 0/1 a 0/12 (10 GbE)
- Cisco Nexus 3232C: Puertos e1/1-30 (40 o 100 u 4 x 10 GbE)

Los switches de clúster utilizan los siguientes puertos de enlace entre switches (ISL).

- NetApp CN1610: Puertos 0/13 a 0/16 (10 GbE)
- Cisco Nexus 3232C: Puertos 1/31-32 (100 GbE)



Debe utilizar 4 cables de arranque de 10 G en el switch de clúster de Cisco Nexus 3232C.

En la siguiente tabla se muestran las conexiones de cableado necesarias en cada fase a medida que se realiza la transición de los switches CN1610 de NetApp a los switches de clúster Cisco Nexus 3232C:

Etapa	Descripción	Cables necesarios
Inicial	CN1610 a CN1610 (SFP+ a SFP+)	4 cables de conexión directa de cobre o fibra óptica SFP+
Transición	CN1610 a 3232C (QSFP a SFP+)	1 cables de cable de fibra óptica o de cobre QSFP y 4 SFP+
Final	3232C a 3232C (QSFP a QSFP)	2 cables de conexión directa de cobre o fibra óptica QSFP

Debe haber descargado los archivos de configuración de referencia (RCF) correspondientes. El número de puertos de 10 GbE y 40/100 GbE se define en los RCF disponibles en la ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) página.

Las versiones ONTAP y NX-OS compatibles con este procedimiento se enumeran en la ["Página Cisco Ethernet Switches"](#).

Las versiones ONTAP Y FASTPATH compatibles con este procedimiento se enumeran en la ["Switches NetApp CN1601 y CN1610"](#).

Requisitos del CN5596

Los switches de clúster utilizan los siguientes puertos para las conexiones a los nodos:

- Puertos e1/1-40 (10 GbE): Nexus 5596
- Puertos e1/1-30 (10/40/100 GbE): Nexus 3232C
 - Los switches de clúster utilizan los siguientes puertos de enlace entre switches (ISL):
- Puertos e1/41-48 (10 GbE): Nexus 5596
- Puertos e1/31-32 (40/100 GbE): Nexus 3232C
 - La ["Hardware Universe"](#) Contiene información sobre el cableado admitido para los switches Nexus 3232C:
- Los nodos con conexiones de clúster de 10 GbE requieren cables de fibra óptica QSFP a SFP+ o cables de cobre QSFP a SFP+.
- Los nodos con conexiones de clúster de 40/100 GbE requieren módulos ópticos QSFP/QSFP28 compatibles con cables de fibra o cables de conexión directa de cobre QSFP/QSFP28.
 - Los switches de clúster utilizan el cableado ISL adecuado:
- Principio: Nexus 5596 (de SFP+ a SFP+)
 - 8 cables de conexión directa de cobre o fibra SFP+
- Provisional: Nexus 5596 a Nexus 3232C (QSFP a 4 partes de SFP+)
 - 1 cables QSFP a SFP+ de fibra óptica o cables de interrupción de cobre

- Final: Nexus 3232C a Nexus 3232C (QSFP28 to QSFP28)

- 2 cables de conexión directa de cobre o fibra QSFP28

- En los switches Nexus 3232C, puede operar puertos QSFP/QSFP28 en modos 40/100 Gigabit Ethernet o 4 x10 Gigabit Ethernet.

De forma predeterminada, hay 32 puertos en el modo 40/100 Gigabit Ethernet. Estos puertos 40 Gigabit Ethernet están numerados en una convención de nomenclatura de 2 tubos. Por ejemplo, el segundo puerto 40 Gigabit Ethernet está numerado como 1/2. El proceso de cambiar la configuración de 40 Gigabit Ethernet a 10 Gigabit Ethernet se denomina *breakout* y el proceso de cambiar la configuración de 10 Gigabit Ethernet a 40 Gigabit Ethernet se denomina *breakin*. Cuando se dividen un puerto 40/100 Gigabit Ethernet en 10 puertos Gigabit Ethernet, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tupla. Por ejemplo, los puertos de salida del segundo puerto Ethernet 40/100 Gigabit están numerados como 1/2/1, 1/2/2, 1/2/3 y 1/2/4.

- En el lado izquierdo de los switches Nexus 3232C son 2 puertos SFP+, que denominan 1/33 y 1/34.
- Ha configurado algunos de los puertos de los switches Nexus 3232C para que se ejecuten a 10 GbE o 40/100 GbE.



Puede dividir los primeros seis puertos en modo 4x10 GbE mediante el interface `breakout module 1 port 1-6 map 10g-4x` comando. De forma similar, puede volver a agrupar los primeros seis puertos QSFP+ de la configuración de cable mediante el `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Ha realizado la planificación, la migración y lea la documentación requerida sobre conectividad de 10 GbE y 40/100 GbE desde los nodos a los switches de clúster de Nexus 3232C.
- Las versiones ONTAP y NX-OS compatibles con este procedimiento son en la "[Página Cisco Ethernet Switches](#)".

Migre un switch de clúster CN1610 a un switch de clúster Cisco Nexus 3232C

Para sustituir los switches de clúster CN1610 existentes en un clúster con switches de clúster Cisco Nexus 3232C, debe realizar una secuencia específica de tareas.

Revise los requisitos

Antes de la migración, asegúrese de revisarla "[Requisitos de migración](#)".



Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Si fuera necesario, consulte lo siguiente para obtener más información:

- "[Página de descripción de NetApp CN1601 y CN1610](#)"
- "[Página de descripción de Cisco Ethernet Switch](#)"
- "[Hardware Universe](#)"

Migrar los switches

Acerca de los ejemplos

Los ejemplos de este procedimiento emplean cuatro nodos: Dos nodos utilizan cuatro puertos de interconexión de clúster de 10 GbE: E0a, e0b, e0c y e0d. Los otros dos nodos utilizan dos cables de fibra de interconexión de clúster de 40 GbE: e4a y e4e. La ["Hardware Universe"](#) tiene información acerca de los cables de fibra de clúster en las plataformas.

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

- Los nodos son n1, n2, n3 y n4.
- Los resultados del comando pueden variar en función de las diferentes versiones del software ONTAP.
- Los interruptores CN1610 que se deben sustituir son CL1 y CL2.
- Los switches Nexus 3232C para sustituir los switches CN1610 son C1 y C2.
- n1_clus1 es la primera interfaz lógica del clúster (LIF) conectada al switch del clúster 1 (CL1 o C1) para el nodo n1.
- n1_clus2 es la primera LIF del clúster que está conectada al switch de clúster 2 (CL2 o C2) para el nodo n1.
- n1_clus3 es la segunda LIF conectada al switch de clúster 2 (CL2 o C2) para el nodo n1.
- n1_clus4 es la segunda LIF conectada al switch de clúster 1 (CL1 o C1) para el nodo n1.
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) página.

Paso 1: Preparación para la migración

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

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

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



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

2. Muestra información sobre los dispositivos de la configuración:

```
network device-discovery show
```

Muestra el ejemplo

El ejemplo siguiente muestra cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster:

```
cluster::> network device-discovery show
```

Node	Local	Discovered		
	Port	Device	Interface	Platform

n1	/cdp			
	e0a	CL1	0/1	CN1610
	e0b	CL2	0/1	CN1610
	e0c	CL2	0/2	CN1610
n2	e0d	CL1	0/2	CN1610
	/cdp			
	e0a	CL1	0/3	CN1610
	e0b	CL2	0/3	CN1610
	e0c	CL2	0/4	CN1610
	e0d	CL1	0/4	CN1610

8 entries were displayed.

3. Determinar el estado administrativo u operativo de cada interfaz de clúster.

a. Muestre los atributos de puerto de red del clúster:

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

Muestra el ejemplo

```
cluster::*> network port show -role cluster
(network port show)
```

Node: n1

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Open	Health Status	Ignore Health
------	---------	------------------	------	-----	----------------------------	---------------	---------------

-----	-----	-----	-----	-----	-----	-----	
-------	-------	-------	-------	-------	-------	-------	--

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n2

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Open	Health Status	Ignore Health
------	---------	------------------	------	-----	----------------------------	---------------	---------------

-----	-----	-----	-----	-----	-----	-----	
-------	-------	-------	-------	-------	-------	-------	--

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	
e0d	cluster	cluster	up	9000	auto/10000	-	

8 entries were displayed.

b. Mostrar información acerca de las interfaces lógicas:

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

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current      Current
Is
Vserver  Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
-----
Cluster
true      n1_clus1    up/up      10.10.0.1/24  n1        e0a
true      n1_clus2    up/up      10.10.0.2/24  n1        e0b
true      n1_clus3    up/up      10.10.0.3/24  n1        e0c
true      n1_clus4    up/up      10.10.0.4/24  n1        e0d
true      n2_clus1    up/up      10.10.0.5/24  n2        e0a
true      n2_clus2    up/up      10.10.0.6/24  n2        e0b
true      n2_clus3    up/up      10.10.0.7/24  n2        e0c
true      n2_clus4    up/up      10.10.0.8/24  n2        e0d

8 entries were displayed.
```

c. Muestra información sobre los switches del clúster detectados:

```
system cluster-switch show
```

Muestra el ejemplo

En el siguiente ejemplo se muestran los switches de clúster que se conocen en el clúster junto con sus direcciones IP de administración:

```
cluster::> system cluster-switch show
```

Switch	Type	Address	Model
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			

2 entries displayed.

4. Verifique que el RCF y la imagen adecuados estén instalados en los nuevos conmutadores 3232C según sea necesario para sus requisitos y realice las personalizaciones esenciales del sitio.

Debe preparar ambos switches en este momento. Si necesita actualizar el RCF y la imagen, debe completar el siguiente procedimiento:

- a. Consulte "[Switch Ethernet de Cisco](#)" En el sitio de soporte de NetApp.
 - b. Anote el conmutador y las versiones de software necesarias en la tabla de esa página.
 - c. Descargue la versión adecuada del RCF.
 - d. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.
 - e. Descargue la versión adecuada del software de imagen en "[Descarga del archivo de configuración de referencia del conmutador de red de administración y clúster Cisco®](#)".
5. Migre los LIF asociados con el segundo switch CN1610 que tiene previsto sustituir:

```
network interface migrate -vserver vservice-name -lif lif-name -source-node  
source-node-name destination-node destination-node-name -destination-port  
destination-port-name
```


Muestra el ejemplo

Debe migrar cada LIF de forma individual, como se muestra en el ejemplo siguiente:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus2
-source-node n1
-destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver cluster -lif n1_clus3
-source-node n1
-destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver cluster -lif n2_clus2
-source-node n2
-destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver cluster -lif n2_clus3
-source-node n2
-destination-node n2 -destination-port e0d
```

6. Compruebe el estado del clúster:

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

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current  Current  Is
Vserver Interface Admin/Oper Address/Mask Node      Port
Home
-----
Cluster
true      n1_clus1    up/up      10.10.0.1/24  n1        e0a
false     n1_clus2    up/up      10.10.0.2/24  n1        e0a
false     n1_clus3    up/up      10.10.0.3/24  n1        e0d
true      n1_clus4    up/up      10.10.0.4/24  n1        e0d
true      n2_clus1    up/up      10.10.0.5/24  n2        e0a
false     n2_clus2    up/up      10.10.0.6/24  n2        e0a
false     n2_clus3    up/up      10.10.0.7/24  n2        e0d
true      n2_clus4    up/up      10.10.0.8/24  n2        e0d

8 entries were displayed.
```

Paso 2: Sustituya el interruptor del grupo CL2 por C2

1. Apague los puertos de interconexión de clúster que estén conectados físicamente al switch CL2:

```
network port modify -node node-name -port port-name -up-admin false
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los cuatro puertos de interconexión de clúster que se están apagando para los nodos n1 y n2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

2. Haga ping a las interfaces remotas del clúster y, a continuación, realice una comprobación del servidor de llamadas de procedimiento remoto:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a      10.10.0.1
Cluster n1_clus2 n1      e0b      10.10.0.2
Cluster n1_clus3 n1      e0c      10.10.0.3
Cluster n1_clus4 n1      e0d      10.10.0.4
Cluster n2_clus1 n2      e0a      10.10.0.5
Cluster n2_clus2 n2      e0b      10.10.0.6
Cluster n2_clus3 n2      e0c      10.10.0.7
Cluster n2_clus4 n2      e0d      10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

3. Apague los puertos ISL 13 a 16 en el conmutador CL1 CN1610 activo con el comando correspondiente.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo, se muestran los puertos ISL 13 a 16 apagados en el switch CN1610 CL1:

```
(CL1)# configure
(CL1) (Config)# interface 0/13-0/16
(CL1) (Interface 0/13-0/16)# shutdown
(CL1) (Interface 0/13-0/16)# exit
(CL1) (Config)# exit
(CL1)#
```

4. Cree un ISL temporal entre CL1 y C2:

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo, se muestra una ISL temporal creada entre CL1 (puertos 13-16) y C2 (puertos e1/24/1-4) mediante Cisco switchport mode trunk comando:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

5. Quite los cables conectados al conmutador CL2 CN1610 en todos los nodos.

Al utilizar el cableado compatible, debe volver a conectar los puertos desconectados de todos los nodos al switch Nexus 3232C C2.

6. Quite cuatro cables ISL de los puertos 13 a 16 en el conmutador CL1 CN1610.

Debe asociar el Cisco QSFP28 adecuado a los cables de arranque SFP+ que conectan el puerto 1/24 del nuevo switch Cisco 3232C C2 a los puertos 13 a 16 en el switch CN1610 existente CL1.



Al volver a conectar cualquier cable al nuevo switch Cisco 3232C, los cables que se utilicen deben ser fibra óptica o cables twinax de Cisco.

7. Configure la interfaz ISL 3/1 en el switch CN1610 activo para desactivar el modo estático.

Esta configuración coincide con la configuración ISL del switch 3232C C2 cuando se configuran los ISL en ambos switches.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el ejemplo siguiente se muestra la interfaz ISL 3/1 que se está configurando para que el ISL sea dinámico:

```
(CL1) # configure
(CL1) (Config) # interface 3/1
(CL1) (Interface 3/1) # no port-channel static
(CL1) (Interface 3/1) # exit
(CL1) (Config) # exit
(CL1) #
```

8. Traiga ISL 13 a 16 en el conmutador CL1 CN1610 activo.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo, se muestran los puertos ISL de 13 a 16 que se están poniendo en marcha en la interfaz puerto-canal de 3/1:

```
(CL1) # configure
(CL1) (Config) # interface 0/13-0/16,3/1
(CL1) (Interface 0/13-0/16,3/1) # no shutdown
(CL1) (Interface 0/13-0/16,3/1) # exit
(CL1) (Config) # exit
(CL1) #
```

9. Compruebe que los ISL son up En el interruptor CL1 CN1610.

El "Estado de enlace" debe ser Up, "Tipo" debe ser Dynamic, Y la columna "Puerto activo" debe ser True para los puertos 0/13 a 0/16.

Muestra el ejemplo

En el ejemplo siguiente se muestran los ISL como verificados up En el conmutador CN1610 CL1:

```
(CL1)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr	Device/	Port	Port
Ports	Timeout	Speed	Active
-----	-----	-----	-----
0/13	actor/long	10 Gb Full	True
	partner/long		
0/14	actor/long	10 Gb Full	True
	partner/long		
0/15	actor/long	10 Gb Full	True
	partner/long		
0/16	actor/long	10 Gb Full	True
	partner/long		

10. Compruebe que los ISL son up En el switch 3232C C2:

```
show port-channel summary
```

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Los puertos eth1/24/1 a eth1/24/4 deben indicarse (P) , Lo que significa que los cuatro puertos ISL están activos en el canal de puerto. Debe indicar eth1/31 y eth1/32 (D) ya que no están conectados.

Muestra el ejemplo

En el ejemplo siguiente se muestran los ISL como verificados up En el switch 3232C C2:

```
C2# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth      LACP      Eth1/31 (D)  Eth1/32 (D)
2      Po2 (SU)       Eth      LACP      Eth1/24/1 (P) Eth1/24/2 (P)
Eth1/24/3 (P)
                                   Eth1/24/4 (P)
```

11. Traigan todos los puertos de interconexión del clúster que están conectados al switch 3232C de todos los nodos:

```
network port modify -node node-name -port port-name -up-admin true
```

Muestra el ejemplo

El siguiente ejemplo muestra cómo traer los puertos de interconexión del clúster conectados al switch 3232C C2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

12. Revierte todos los LIF de interconexión del clúster migrados que están conectados a C2 en todos los nodos:

```
network interface revert -vserver cluster -lif lif-name
```


Muestra el ejemplo

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2
cluster::*> network interface revert -vserver cluster -lif n1_clus3
cluster::*> network interface revert -vserver cluster -lif n2_clus2
cluster::*> network interface revert -vserver cluster -lif n2_clus3
```

13. Compruebe que todos los puertos de interconexión de clúster se hayan revertido a sus puertos principales:

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

Muestra el ejemplo

En el ejemplo siguiente se muestra que las LIF en clus2 se revierten a sus puertos raíz; las LIF se revierten correctamente si el estado de los puertos de la columna "puerto actual" es `true` En la columna "es de inicio". Si el valor "es de casa" es `false`, Entonces el LIF no se revierte.

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current      Current      Is
Vserver Interface Admin/Oper Address/Mask Node      Port
Home
-----
Cluster
true      n1_clus1      up/up      10.10.0.1/24      n1      e0a
true      n1_clus2      up/up      10.10.0.2/24      n1      e0b
true      n1_clus3      up/up      10.10.0.3/24      n1      e0c
true      n1_clus4      up/up      10.10.0.4/24      n1      e0d
true      n2_clus1      up/up      10.10.0.5/24      n2      e0a
true      n2_clus2      up/up      10.10.0.6/24      n2      e0b
true      n2_clus3      up/up      10.10.0.7/24      n2      e0c
true      n2_clus4      up/up      10.10.0.8/24      n2      e0d

8 entries were displayed.
```

14. Compruebe que todos los puertos del clúster estén conectados:

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

Muestra el ejemplo

En el siguiente ejemplo, se muestra el resultado de verificar que todas las interconexiones del clúster sean up:

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

```
(network port show)
```

Node: n1

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Open	Health Status	Ignore Health
e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n2

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Open	Health Status	Ignore Health
e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	
e0d	cluster	cluster	up	9000	auto/10000	-	

8 entries were displayed.

15. Haga ping a las interfaces remotas del clúster y, a continuación, realice una comprobación del servidor de llamadas de procedimiento remoto:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a      10.10.0.1
Cluster n1_clus2 n1      e0b      10.10.0.2
Cluster n1_clus3 n1      e0c      10.10.0.3
Cluster n1_clus4 n1      e0d      10.10.0.4
Cluster n2_clus1 n2      e0a      10.10.0.5
Cluster n2_clus2 n2      e0b      10.10.0.6
Cluster n2_clus3 n2      e0c      10.10.0.7
Cluster n2_clus4 n2      e0d      10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

16. Migre las LIF asociadas con el primer switch CL1 CN1610:

```
network interface migrate -vserver cluster -lif lif-name -source-node node-name
```

Muestra el ejemplo

Debe migrar cada LIF del clúster de forma individual a los puertos de clúster adecuados alojados en el switch del clúster C2, como se muestra en el ejemplo siguiente:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus1
-source-node n1
-destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver cluster -lif n1_clus4
-source-node n1
-destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver cluster -lif n2_clus1
-source-node n2
-destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver cluster -lif n2_clus4
-source-node n2
-destination-node n2 -destination-port e0c
```

Paso 3: Sustituya el interruptor del grupo de instrumentos CL1 por C1

1. Compruebe el estado del clúster:

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

Muestra el ejemplo

El siguiente ejemplo muestra que las LIF de clúster necesarias se han migrado a los puertos de clúster correspondientes alojados en el switch de clúster C2:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current  Current  Is
Vserver Interface Admin/Oper Address/Mask Node      Port
Home
-----
-----
Cluster
false      n1_clus1    up/up      10.10.0.1/24  n1        e0b
true       n1_clus2    up/up      10.10.0.2/24  n1        e0b
true       n1_clus3    up/up      10.10.0.3/24  n1        e0c
false      n1_clus4    up/up      10.10.0.4/24  n1        e0c
false      n2_clus1    up/up      10.10.0.5/24  n2        e0b
false      n2_clus2    up/up      10.10.0.6/24  n2        e0b
true       n2_clus3    up/up      10.10.0.7/24  n2        e0c
true       n2_clus4    up/up      10.10.0.8/24  n2        e0c
false

8 entries were displayed.
```

2. Apague los puertos de nodo que estén conectados a CL1 en todos los nodos:

```
network port modify -node node-name -port port-name -up-admin false
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran puertos específicos que se están apagando en los nodos n1 y n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

3. Apague los puertos ISL 24, 31 y 32 en el switch 3232C activo C2.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo se muestran los ISL 24, 31 y 32 apagados en el switch 3232C activo C2:

```
C2# configure
C2(config)# interface ethernet 1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
C2#
```

4. Quite los cables conectados al conmutador CL1 CN1610 de todos los nodos.

Al utilizar el cableado apropiado, debe volver a conectar los puertos desconectados de todos los nodos al switch Nexus 3232C C1.

5. Quite los cables QSFP28 del puerto Nexus 3232C C2 e1/24.

Debe conectar los puertos e1/31 y e1/32 en C1 a los puertos e1/31 y e1/32 en C2 mediante los cables de fibra óptica Cisco QSFP28 o de conexión directa admitidos.

6. Restaure la configuración en el puerto 24 y retire el canal de puerto temporal 2 en C2:

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo se muestra el running-configuration archivo que se copia en startup-configuration archivo:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# interface e1/24
C2(config-if)# description 100GbE/40GbE Node Port
C2(config-if)# spanning-tree port type edge
Edge port type (portfast) should only be enabled on ports connected
to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet 1/24 but
will only
have effect when the interface is in a non-trunking mode.

C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

7. Suba los puertos ISL 31 y 32 en C2, el switch 3232C activo.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

El siguiente ejemplo muestra que se trajeron ISL 31 y 32 al switch 3232C C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

8. Compruebe que las conexiones ISL están up En el conmutador C2 3232C.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo, se muestran las conexiones ISL que se están verificando. Los puertos eth1/31 y eth1/32 se indican (P) , Lo que significa que ambos puertos ISL son up en el puerto-canal:

```
C1# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        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)
```

```
C2# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        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)
```

9. Traiga todos los puertos de interconexión del clúster conectados al nuevo switch C1 de 3232C en todos los nodos:

```
network port modify -node node-name -port port-name -up-admin true
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran todos los puertos de interconexión del clúster conectados al nuevo switch C1 que se está subiendo:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

10. Compruebe el estado del puerto del nodo del clúster:

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

Muestra el ejemplo

En el siguiente ejemplo se muestra un resultado que comprueba que los puertos de interconexión del clúster en los nodos n1 y n2 del nuevo switch 3232C C1 up:

```
cluster::*> network port show -role cluster
(network port show)

Node: n1

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Admin/Open  Status  Health
-----
-----
e0a    cluster  cluster    up    9000  auto/10000    -
e0b    cluster  cluster    up    9000  auto/10000    -
e0c    cluster  cluster    up    9000  auto/10000    -    -
e0d    cluster  cluster    up    9000  auto/10000    -    -

Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Admin/Open  Status  Health
-----
-----
e0a    cluster  cluster    up    9000  auto/10000    -
e0b    cluster  cluster    up    9000  auto/10000    -
e0c    cluster  cluster    up    9000  auto/10000    -
e0d    cluster  cluster    up    9000  auto/10000    -

8 entries were displayed.
```

Paso 4: Complete el procedimiento

1. Revierte todos los LIF de interconexión del clúster migrados que estaban conectados originalmente a C1 en todos los nodos:

```
network interface revert -server cluster -lif lif-name
```

Muestra el ejemplo

Debe migrar cada LIF de forma individual, como se muestra en el ejemplo siguiente:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n1_clus4
cluster::*> network interface revert -vserver cluster -lif n2_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus4
```

2. Compruebe que la interfaz se encuentra ahora en casa:

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

Muestra el ejemplo

En el ejemplo siguiente se muestra el estado de las interfaces de interconexión del clúster es up Y "es Home" para los nodos n1 y n2:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current  Current  Is
Vserver Interface Admin/Oper Address/Mask Node      Port
Home
-----
-----
Cluster
true      n1_clus1    up/up      10.10.0.1/24  n1        e0a
true      n1_clus2    up/up      10.10.0.2/24  n1        e0b
true      n1_clus3    up/up      10.10.0.3/24  n1        e0c
true      n1_clus4    up/up      10.10.0.4/24  n1        e0d
true      n2_clus1    up/up      10.10.0.5/24  n2        e0a
true      n2_clus2    up/up      10.10.0.6/24  n2        e0b
true      n2_clus3    up/up      10.10.0.7/24  n2        e0c
true      n2_clus4    up/up      10.10.0.8/24  n2        e0d
true

8 entries were displayed.
```

3. Haga ping a las interfaces remotas del clúster y, a continuación, realice una comprobación del servidor de llamadas de procedimiento remoto:

```
cluster ping-cluster -node host-name
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
3  paths up, 0 paths down (udp check)
```

4. Expanda el clúster añadiendo nodos a los switches de clúster Nexus 3232C.

5. Muestra la información sobre los dispositivos de la configuración:

- ° `network device-discovery show`
- ° `network port show -role cluster`
- ° `network interface show -role cluster`
- ° `system cluster-switch show`

Muestra el ejemplo

En los siguientes ejemplos se muestran los nodos n3 y n4 con puertos de clúster de 40 GbE conectados a los puertos e1/7 y e1/8, respectivamente, en los dos switches de clúster Nexus 3232C. Ambos nodos están Unidos al clúster. Los puertos de interconexión de clúster de 40 GbE utilizados son e4a y e4e.

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform

n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

12 entries were displayed.

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

```
(network port show)
```

```
Node: n1
```

		Broadcast			Speed (Mbps)	Health
Ignore						
Port	IPspace	Domain	Link	MTU	Admin/Open	Status
Health	Status					

e0a	cluster	cluster	up	9000	auto/10000	-
e0b	cluster	cluster	up	9000	auto/10000	-
e0c	cluster	cluster	up	9000	auto/10000	-
e0d	cluster	cluster	up	9000	auto/10000	-

Node: n2

		Broadcast			Speed (Mbps)	Health
Ignore						
Port	IPspace	Domain	Link	MTU	Admin/Open	Status
Health	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e0a	cluster	cluster	up	9000	auto/10000	-
e0b	cluster	cluster	up	9000	auto/10000	-
e0c	cluster	cluster	up	9000	auto/10000	-
e0d	cluster	cluster	up	9000	auto/10000	-

Node: n3

		Broadcast			Speed (Mbps)	Health
Ignore						
Port	IPspace	Domain	Link	MTU	Admin/Open	Status
Health	Status					
-----	-----	-----	-----	-----	-----	-----
e4a	cluster	cluster	up	9000	auto/40000	-
e4e	cluster	cluster	up	9000	auto/40000	-

Node: n4

		Broadcast			Speed (Mbps)	Health
Ignore						
Port	IPspace	Domain	Link	MTU	Admin/Open	Status
Health	Status					
-----	-----	-----	-----	-----	-----	-----
e4a	cluster	cluster	up	9000	auto/40000	-
e4e	cluster	cluster	up	9000	auto/40000	-

12 entries were displayed.

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

(network interface show)

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

Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true	n1_clus2	up/up	10.10.0.2/24	n1	e0b

```

true
      n1_clus3   up/up      10.10.0.3/24   n1      e0c
true
      n1_clus4   up/up      10.10.0.4/24   n1      e0d
true
      n2_clus1   up/up      10.10.0.5/24   n2      e0a
true
      n2_clus2   up/up      10.10.0.6/24   n2      e0b
true
      n2_clus3   up/up      10.10.0.7/24   n2      e0c
true
      n2_clus4   up/up      10.10.0.8/24   n2      e0d
true
      n3_clus1   up/up      10.10.0.9/24   n3      e4a
true
      n3_clus2   up/up      10.10.0.10/24  n3      e4e
true
      n4_clus1   up/up      10.10.0.11/24  n4      e4a
true
      n4_clus2   up/up      10.10.0.12/24  n4      e4e
true

```

12 entries were displayed.

cluster::> **system cluster-switch show**

Switch	Type	Address	Model
C1	cluster-network	10.10.1.103	
NX3232C			
Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP			

C2	cluster-network	10.10.1.104	
NX3232C			

Serial Number: FOX000002
 Is Monitored: true
 Reason:

```

    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    7.0(3)I6(1)
    Version Source: CDP
CL1                cluster-network  10.10.1.101    CN1610

    Serial Number: 01234567
    Is Monitored: true
    Reason:
    Software Version: 1.2.0.7
    Version Source: ISDP
CL2                cluster-network  10.10.1.102
CN1610

    Serial Number: 01234568
    Is Monitored: true
    Reason:
    Software Version: 1.2.0.7
    Version Source: ISDP 4 entries were displayed.

```

6. Extraiga los interruptores CN1610 sustituidos si no se retiran automáticamente:

```
system cluster-switch delete -device switch-name
```

Muestra el ejemplo

Debe eliminar ambos dispositivos individualmente, como se muestra en el siguiente ejemplo:

```

cluster::> system cluster-switch delete -device CL1
cluster::> system cluster-switch delete -device CL2

```

7. Compruebe que se supervisan los switches de clúster adecuados:

```
system cluster-switch show
```

Muestra el ejemplo

En el siguiente ejemplo se muestran los switches del clúster C1 y C2 que se están supervisando:

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.104
Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP		

2 entries were displayed.

8. Habilitar la función de recopilación de registros del monitor de estado del switch de clúster para recopilar archivos de registro relacionados con el conmutador:

```
system cluster-switch log setup-password
```

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

Muestra el ejemplo

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

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

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

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

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

Enabling cluster switch log collection.

cluster::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

9. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

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

Migre de un switch de clúster Cisco Nexus 5596 a un switch de clúster Cisco Nexus 3232C

Siga este procedimiento para migrar un switch de clúster Cisco Nexus 5596 existente en un clúster con switches de clúster Nexus 3232C.

Revise los requisitos

Antes de la migración, asegúrese de revisarla ["Requisitos de migración"](#).



Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Para obtener más información, consulte:

- ["Página de descripción de Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Migrar el switch

Acerca de los ejemplos

Los ejemplos de este procedimiento describen el reemplazo de los switches Cisco Nexus 5596 por switches Cisco Nexus 3232C. Puede utilizar estos pasos (con modificaciones) para otros conmutadores Cisco antiguos (por ejemplo, 3132Q-V).

El procedimiento también utiliza la siguiente nomenclatura de conmutación y nodo:

- Los resultados del comando pueden variar en función de las diferentes versiones de ONTAP.
- Los interruptores Nexus 5596 que se deben sustituir son CL1 y CL2.
- Los switches Nexus 3232C para sustituir los switches Nexus 5596 son C1 y C2.
- n1_clus1 es la primera interfaz lógica del clúster (LIF) conectada al switch del clúster 1 (CL1 o C1) para el nodo n1.
- n1_clus2 es la primera LIF del clúster conectada al switch de clúster 2 (CL2 o C2) para el nodo n1.
- n1_clus3 es la segunda LIF conectada al switch de clúster 2 (CL2 o C2) para el nodo n1.
- n1_clus4 es la segunda LIF conectada al switch de clúster 1 (CL1 o C1) para el nodo n1.-
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) página.
- Los nodos son n1, n2, n3 y n4.

Los ejemplos de este procedimiento utilizan cuatro nodos:

- Dos nodos utilizan cuatro puertos de interconexión de clúster de 10 GbE: E0a, e0b, e0c y e0d.
- Los otros dos nodos utilizan dos puertos de interconexión de clúster de 40 GbE: e4a y e4e. La ["Hardware Universe"](#) la enumera los puertos del clúster reales en las plataformas.

Escenarios

Este procedimiento cubre los siguientes escenarios:

- El clúster comienza con dos nodos conectados y funcionan en dos switches de clúster Nexus 5596.

- El switch del clúster CL2 debe sustituirse por C2 (pasos del 1 al 19):
 - El tráfico de todos los puertos del clúster y las LIF de todos los nodos conectados a CL2 se migran a los primeros puertos del clúster y las LIF conectadas a CL1.
 - Desconecte el cableado de todos los puertos del clúster de todos los nodos conectados a CL2 y, a continuación, utilice un cableado de desconexión compatible para volver a conectar los puertos al nuevo switch de clúster C2.
 - Desconecte el cableado entre los puertos ISL entre CL1 y CL2 y, a continuación, utilice el cableado de desconexión admitido para volver a conectar los puertos de CL1 a C2.
 - Se revierte el tráfico en todos los puertos del clúster y los LIF conectados a C2 en todos los nodos.
- El switch del clúster CL2 se debe sustituir por C2.
 - El tráfico de todos los puertos de clúster o las LIF de todos los nodos conectados a CL1 se migran a los segundos puertos de clúster o las LIF conectadas a C2.
 - Desconecte el cableado de todos los puertos del clúster de todos los nodos conectados a CL1 y vuelva a conectarlo, mediante el cableado de desconexión compatible, al nuevo switch del clúster C1.
 - Desconecte el cableado entre los puertos ISL entre CL1 y C2 y vuelva a conectarse mediante el cableado compatible, de C1 a C2.
 - Se revierte el tráfico en todos los puertos del clúster o LIF conectados a C1 en todos los nodos.
- Se han añadido dos nodos FAS9000 al clúster con ejemplos que muestran los detalles del clúster.

Paso 1: Preparación para la migración

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

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

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



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

2. Muestra información sobre los dispositivos de la configuración:

```
network device-discovery show
```


Muestra el ejemplo

En el ejemplo siguiente se muestra cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster:

```
cluster::> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform
-----	-----	-----	-----	-----
n1	/cdp			
	e0a	CL1	Ethernet1/1	N5K-C5596UP
	e0b	CL2	Ethernet1/1	N5K-C5596UP
	e0c	CL2	Ethernet1/2	N5K-C5596UP
	e0d	CL1	Ethernet1/2	N5K-C5596UP
n2	/cdp			
	e0a	CL1	Ethernet1/3	N5K-C5596UP
	e0b	CL2	Ethernet1/3	N5K-C5596UP
	e0c	CL2	Ethernet1/4	N5K-C5596UP
	e0d	CL1	Ethernet1/4	N5K-C5596UP

8 entries were displayed.

3. Determinar el estado administrativo u operativo de cada interfaz de clúster.

a. Mostrar los atributos del puerto de red:

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

Muestra el ejemplo

En el ejemplo siguiente se muestran los atributos de puerto de red en los nodos n1 y n2:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e0a         Cluster      Cluster      up    9000 auto/10000 -
-
e0b         Cluster      Cluster      up    9000 auto/10000 -
-
e0c         Cluster      Cluster      up    9000 auto/10000 -
-
e0d         Cluster      Cluster      up    9000 auto/10000 -
-

Node: n2

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e0a         Cluster      Cluster      up    9000 auto/10000 -
-
e0b         Cluster      Cluster      up    9000 auto/10000 -
-
e0c         Cluster      Cluster      up    9000 auto/10000 -
-
e0d         Cluster      Cluster      up    9000 auto/10000 -
-
8 entries were displayed.
```

b. Mostrar información acerca de las interfaces lógicas:

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

Muestra el ejemplo

En el ejemplo siguiente se muestra la información general sobre todas las LIF del clúster, incluidos sus puertos actuales:

```
cluster::*> network interface show -role cluster
(network interface show)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e0a true n1_clus1 up/up 10.10.0.1/24 n1
e0b true n1_clus2 up/up 10.10.0.2/24 n1
e0c true n1_clus3 up/up 10.10.0.3/24 n1
e0d true n1_clus4 up/up 10.10.0.4/24 n1
e0a true n2_clus1 up/up 10.10.0.5/24 n2
e0b true n2_clus2 up/up 10.10.0.6/24 n2
e0c true n2_clus3 up/up 10.10.0.7/24 n2
e0d true n2_clus4 up/up 10.10.0.8/24 n2
8 entries were displayed.
```

c. Muestra información sobre los switches del clúster detectados:

```
system cluster-switch show
```

Muestra el ejemplo

En el siguiente ejemplo se muestran los switches de clúster activos:

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX5596	cluster-network	10.10.1.101
Serial Number: 01234567		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.1(1)N1(1)		
Version Source: CDP		
CL2 NX5596	cluster-network	10.10.1.102
Serial Number: 01234568		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.1(1)N1(1)		
Version Source: CDP		

2 entries were displayed.

4. Compruebe que el RCF y la imagen adecuados están instalados en los nuevos conmutadores 3232C según sea necesario para sus requisitos y realice las personalizaciones esenciales del sitio, como usuarios y contraseñas, direcciones de red y otras personalizaciones.



Debe preparar ambos switches en este momento.

Si necesita actualizar el RCF y la imagen, debe realizar los siguientes pasos:

- a. Vaya a la página *Cisco Ethernet Switches* del sitio de soporte de NetApp.

["Switches Ethernet de Cisco"](#)

- b. Anote el conmutador y las versiones de software necesarias en la tabla de esa página.
- c. Descargue la versión adecuada del RCF.
- d. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación,

siga las instrucciones de la página **Descargar** para descargar el RCF.

e. Descargue la versión adecuada del software Image.

Consulte la página *ONTAP 8.x o posterior Archivos de configuración de referencia de switches de red de administración y clúster* Descargar y, a continuación, haga clic en la versión adecuada.

Para encontrar la versión correcta, consulte la *ONTAP 8.x o posterior página de descarga del conmutador de red de clúster*.

5. Migre los LIF asociados con el segundo switch Nexus 5596 que se va a reemplazar:

```
network interface migrate -vserver vservice-name -lif lif-name -source-node
source-node-name - destination-node node-name -destination-port destination-
port-name
```

Muestra el ejemplo

El ejemplo siguiente muestra las LIF que se están migrando para los nodos n1 y n2; la migración de LIF se debe realizar en todos los nodos:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -
destination-node n2 -destination-port e0d
```

6. Compruebe el estado del clúster:

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

Muestra el ejemplo

En el ejemplo siguiente se muestra el estado actual de cada clúster:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
-----
Cluster
e0a          n1_clus1    up/up      10.10.0.1/24      n1
true
e0a          n1_clus2    up/up      10.10.0.2/24      n1
false
e0d          n1_clus3    up/up      10.10.0.3/24      n1
false
e0d          n1_clus4    up/up      10.10.0.4/24      n1
true
e0a          n2_clus1    up/up      10.10.0.5/24      n2
true
e0a          n2_clus2    up/up      10.10.0.6/24      n2
false
e0d          n2_clus3    up/up      10.10.0.7/24      n2
false
e0d          n2_clus4    up/up      10.10.0.8/24      n2
true
8 entries were displayed.
```

Paso 2: Configurar puertos

1. Apague los puertos de interconexión de clúster que estén conectados físicamente al switch CL2:

```
network port modify -node node-name -port port-name -up-admin false
```

Muestra el ejemplo

Los siguientes comandos apagan los puertos especificados en n1 y n2, pero los puertos deben estar apagados en todos los nodos:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

2. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```


3. Apague ISL 41 a 48 en CL1, el switch Nexus 5596 activo con Cisco `shutdown` comando.

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

Muestra el ejemplo

En el ejemplo siguiente se muestran los ISL 41 a 48 apagados en el switch Nexus 5596 CL1:

```
(CL1) # configure
(CL1) (Config) # interface e1/41-48
(CL1) (config-if-range) # shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

4. Cree un ISL temporal entre CL1 y C2 con los comandos de Cisco correspondientes.

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

Muestra el ejemplo

En el siguiente ejemplo, se muestra una configuración de ISL temporal entre CL1 y C2:

```
C2# configure
C2(config) # interface port-channel 2
C2(config-if) # switchport mode trunk
C2(config-if) # spanning-tree port type network
C2(config-if) # mtu 9216
C2(config-if) # interface breakout module 1 port 24 map 10g-4x
C2(config) # interface e1/24/1-4
C2(config-if-range) # switchport mode trunk
C2(config-if-range) # mtu 9216
C2(config-if-range) # channel-group 2 mode active
C2(config-if-range) # exit
C2(config-if) # exit
```

5. En todos los nodos, quite todos los cables conectados al switch CL2 Nexus 5596.

Con el cableado compatible, vuelva a conectar los puertos desconectados de todos los nodos al switch Nexus 3232C C2.

6. Retire todos los cables del conmutador Nexus 5596 CL2.

Conecte los cables de ruptura Cisco QSFP a SFP+ que conectan el puerto 1/24 del nuevo switch Cisco

3232C, C2, a los puertos 45 a 48 en Nexus 5596, CL1 existente.

7. Traiga los puertos ISL 45 a 48 en el switch CL1 de Nexus 5596 activo.

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

Muestra el ejemplo

El ejemplo siguiente muestra los puertos ISL 45 a 48 que se están poniendo en marcha:

```
(CL1) # configure
(CL1) (Config) # interface e1/45-48
(CL1) (config-if-range) # no shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

8. Compruebe que los ISL son up En el interruptor Nexus 5596 CL1.

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

Muestra el ejemplo

En el siguiente ejemplo, se muestran los puertos eth1/45 a eth1/48 con el significado de (P), lo que significa que los puertos ISL se encuentran up en el puerto-canal.

```
CL1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth      LACP      Eth1/41 (D)  Eth1/42 (D)
Eth1/43 (D)
                                   Eth1/44 (D)  Eth1/45 (P)
Eth1/46 (P)
                                   Eth1/47 (P)  Eth1/48 (P)
```

9. Compruebe que las interfaces eth1/45-48 ya tienen "modo de grupo de canal 1 activo" en su configuración de ejecución.
10. En todos los nodos, obtenga todos los puertos de interconexión del clúster conectados al switch 3232C C2:

```
network port modify -node node-name -port port-name -up-admin true
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran los puertos especificados que se están up en los nodos n1 y n2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

11. En todos los nodos, revierte todos los LIF de interconexión del clúster migrados conectados a C2:

```
network interface revert -vserver Cluster -lif lif-name
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los LIF de clúster migrados que se han revertido a sus puertos principales:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

12. Verifique que todos los puertos de interconexión de clúster ahora se reviertan a su origen:

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

Muestra el ejemplo

En el ejemplo siguiente se muestra que las LIF en clus2 se han revertido a sus puertos raíz y se muestra que las LIF se han revertido correctamente si los puertos de la columna de puerto actual tienen el estado de `true` en la `Is Home` columna. Si la `Is Home` el valor es `false`, El LIF no se ha revertido.

```
cluster::*> *network interface show -role cluster*
(network interface show)
      Logical   Status   Network   Current
Current Is
Vserver      Interface Admin/Oper Address/Mask   Node
Port        Home
-----
Cluster
      n1_clus1   up/up    10.10.0.1/24   n1
e0a    true
      n1_clus2   up/up    10.10.0.2/24   n1
e0b    true
      n1_clus3   up/up    10.10.0.3/24   n1
e0c    true
      n1_clus4   up/up    10.10.0.4/24   n1
e0d    true
      n2_clus1   up/up    10.10.0.5/24   n2
e0a    true
      n2_clus2   up/up    10.10.0.6/24   n2
e0b    true
      n2_clus3   up/up    10.10.0.7/24   n2
e0c    true
      n2_clus4   up/up    10.10.0.8/24   n2
e0d    true
8 entries were displayed.
```

13. Compruebe que los puertos del clúster están conectados:

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

Muestra el ejemplo

En el siguiente ejemplo se muestra el resultado del anterior `network port modify` comando, comprobando que todas las interconexiones del clúster lo son up:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a       Cluster      Cluster      up    9000  auto/10000  -
-
e0b       Cluster      Cluster      up    9000  auto/10000  -
-
e0c       Cluster      Cluster      up    9000  auto/10000  -
-
e0d       Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a       Cluster      Cluster      up    9000  auto/10000  -
-
e0b       Cluster      Cluster      up    9000  auto/10000  -
-
e0c       Cluster      Cluster      up    9000  auto/10000  -
-
e0d       Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

14. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```


15. En cada nodo del clúster, migre las interfaces asociadas con el primer switch Nexus 5596, CL1, que se sustituirá:

```
network interface migrate -vserver vservice-name -lif lif-name -source-node
source-node-name -destination-node destination-node-name -destination-port
destination-port-name
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos o las LIF que se están migrando en los nodos n1 y n2:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-source-node n1 -
destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-source-node n1 -
destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-source-node n2 -
destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-source-node n2 -
destination-node n2 -destination-port e0c
```

16. Compruebe el estado del clúster:

```
network interface show
```

Muestra el ejemplo

El siguiente ejemplo muestra que las LIF de clúster necesarias se han migrado a puertos de clúster adecuados alojados en el switch de clúster, C2:

```
cluster::*> network interface show
```

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

Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0b	false			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0c	false			
	n2_clus1	up/up	10.10.0.5/24	n2
e0b	false			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0c	false			
8 entries were displayed.				

17. En todos los nodos, apague los puertos de nodo que estén conectados a CL1:

```
network port modify -node node-name -port port-name -up-admin false
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos especificados que se están apagando en los nodos n1 y n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

18. Apague ISL 24, 31 y 32 en el interruptor activo 3232C C2.

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

Muestra el ejemplo

El ejemplo siguiente muestra que los ISL se están cerrando:

```
C2# configure
C2(Config)# interface e1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if)# exit
C2#
```

19. En todos los nodos, quite todos los cables conectados al switch CL1 Nexus 5596.

Con el cableado compatible, vuelva a conectar los puertos desconectados de todos los nodos al switch Nexus 3232C C1.

20. Quite el cable de arranque QSFP de los puertos Nexus 3232C C2 e1/24.

Conecte los puertos e1/31 y e1/32 en C1 a los puertos e1/31 y e1/32 en C2 utilizando cables de fibra óptica Cisco QSFP o de conexión directa compatibles.

21. Restaure la configuración en el puerto 24 y retire el canal de puerto temporal 2 en C2.

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

Muestra el ejemplo

En el ejemplo siguiente se muestra la configuración del puerto m24 que se está restaurando utilizando los comandos de Cisco correspondientes:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

22. Traiga los puertos ISL 31 y 32 en C2, el switch 3232C activo, introduciendo el siguiente comando de Cisco: `no shutdown`

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

Muestra el ejemplo

En el siguiente ejemplo se muestran los comandos de Cisco `switchname configure` Se sube en el switch 3232C C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
```

23. Compruebe que las conexiones ISL están up En el conmutador C2 3232C.

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

Los puertos eth1/31 y eth1/32 deben indicar (P) esto con el significado de ambos puertos ISL se deben subir en el puerto-canal

Muestra el ejemplo

```
C1# 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
      S - Switched        R - Routed
      U - Up (port-channel)
      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)
```

24. En todos los nodos, obtenga todos los puertos de interconexión del clúster conectados al nuevo switch 3232C C1:

```
network port modify
```

Muestra el ejemplo

En el siguiente ejemplo se muestran todos los puertos de interconexión de clúster que se están creando para n1 y n2 en el switch 3232C C1:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

25. Compruebe el estado del puerto del nodo del clúster:

```
network port show
```

Muestra el ejemplo

En el siguiente ejemplo, se muestra que todos los puertos de interconexión del clúster de todos los nodos del nuevo switch C1 3232C están activos:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

26. En todos los nodos, revierte los LIF de clúster específicos a sus puertos de inicio:

```
network interface revert -server Cluster -lif lif-name
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los LIF de clúster específicos que se están reteniendo a sus puertos raíz en los nodos n1 y n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1  
cluster::*> network interface revert -vserver Cluster -lif n1_clus4  
cluster::*> network interface revert -vserver Cluster -lif n2_clus1  
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

27. Compruebe que la interfaz es la principal:

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

Muestra el ejemplo

En el ejemplo siguiente se muestra el estado de las interfaces de interconexión de clúster son up y..
Is Home para n1 y n2:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0b      true
      n1_clus3      up/up      10.10.0.3/24      n1
e0c      true
      n1_clus4      up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1      up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2      up/up      10.10.0.6/24      n2
e0b      true
      n2_clus3      up/up      10.10.0.7/24      n2
e0c      true
      n2_clus4      up/up      10.10.0.8/24      n2
e0d      true
8 entries were displayed.
```

28. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster -node node-name
```


Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

29. Expanda el clúster añadiendo nodos a los switches de clúster Nexus 3232C.

En los siguientes ejemplos se muestran los nodos n3 y n4 tienen puertos de clúster de 40 GbE conectados a los puertos e1/7 y e1/8 respectivamente en los dos switches de clúster Nexus 3232C, y ambos nodos se han Unido al clúster. Los puertos de interconexión de clúster de 40 GbE utilizados son e4a y e4e.

Muestra la información sobre los dispositivos de la configuración:

- ° `network device-discovery show`
- ° `network port show -role cluster`
- ° `network interface show -role cluster`
- ° `system cluster-switch show`

Muestra el ejemplo

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

12 entries were displayed.

+

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

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Speed(Mbps)	Health Status
	e0a	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0b	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0c	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0d	Cluster	Cluster	up	9000	auto/10000	-	

```

-

Node: n2

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000 -
-
e0b        Cluster      Cluster      up    9000  auto/10000 -
-
e0c        Cluster      Cluster      up    9000  auto/10000 -
-
e0d        Cluster      Cluster      up    9000  auto/10000 -
-

Node: n3

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a        Cluster      Cluster      up    9000  auto/40000 -
-
e4e        Cluster      Cluster      up    9000  auto/40000 -
-

Node: n4

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a        Cluster      Cluster      up    9000  auto/40000 -
-
e4e        Cluster      Cluster      up    9000  auto/40000 -

```

-
12 entries were displayed.

+

```
cluster::*> network interface show -role cluster
(network interface show)
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

12 entries were displayed.

+

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
CL1 NX5596	cluster-network	10.10.1.101
Serial Number: 01234567		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.1(1)N1(1)		
Version Source: CDP		
CL2 NX5596	cluster-network	10.10.1.102
Serial Number: 01234568		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.1(1)N1(1)		
Version Source: CDP		

```
4 entries were displayed.
```

30. Retire el Nexus 5596 sustituido mediante el `system cluster-switch delete` si no se quita automáticamente:

```
system cluster-switch delete -device switch-name
```

Muestra el ejemplo

```
cluster::> system cluster-switch delete -device CL1  
cluster::> system cluster-switch delete -device CL2
```

Paso 3: Complete el procedimiento

1. Compruebe que se supervisan los switches de clúster adecuados:

```
system cluster-switch show
```

Muestra el ejemplo

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
C1 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

2. Habilite la función de recogida de registro de supervisión del estado del switch para recopilar archivos de registro relacionados con el switch:

```
system cluster-switch log setup-password
```

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


Muestra el ejemplo

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

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

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

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

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

Enabling cluster switch log collection.

cluster::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

3. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

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

Migre de un clúster sin switches de dos nodos a un clúster con switches de clúster Cisco Nexus 3232C

Si tiene un clúster *sin switch* de dos nodos, puede migrar a un clúster *switch* de dos nodos que incluya los switches de red de clústeres Cisco Nexus 3232C. Se trata de un procedimiento no disruptivo.

Revise los requisitos

Requisitos de migración

Antes de la migración, asegúrese de revisarla ["Requisitos de migración"](#).

Lo que necesitará

Asegúrese de que:

- Los puertos están disponibles para las conexiones de nodos. Los switches de clúster utilizan los puertos de enlace entre switches (ISL) e1/31-32.
- Tiene los cables adecuados para las conexiones del clúster:
 - Los nodos con conexiones de clúster de 10 GbE requieren módulos ópticos QSFP con cables de fibra de cable de cable de cobre QSFP a SFP+.
 - Los nodos con conexiones de clúster de 40/100 GbE requieren el soporte de módulos ópticos QSFP/QSFP28 con cables de fibra o cables de conexión directa de cobre QSFP/QSFP28.
 - Los switches de clúster requieren el cableado ISL apropiado: 2 cables de conexión directa de cobre o fibra QSFP28.
- Las configuraciones están correctamente configuradas y funcionan.

Los dos nodos deben estar conectados y funcionar en un valor de clúster sin switch de dos nodos.

- Todos los puertos del clúster están en el estado **up**.
- Se admite el switch de clúster Cisco Nexus 3232C.
- La configuración de red del clúster existente tiene lo siguiente:
 - Infraestructura de clúster Nexus 3232C redundante y totalmente funcional en ambos switches
 - Las versiones más recientes de RCF y NX-OS en sus switches
 - Conectividad de gestión en ambos switches
 - Acceso de consola a ambos switches
 - Todas las interfaces lógicas de clúster (LIF) en el estado **up** sin haber sido migradas
 - Personalización inicial del conmutador
 - Todos los puertos ISL habilitados y cableado

Migrar los switches

Acerca de los ejemplos

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

- Switches de clúster Nexus 3232C, C1 y C2.

- Los nodos son n1 y n2.

Los ejemplos de este procedimiento utilizan dos nodos, cada uno utilizando dos puertos de interconexión de clúster de 40 GbE e4a y e4e. La "[Hardware Universe](#)" tiene detalles acerca de los puertos de clúster en las plataformas.

- n1_clus1 es la primera interfaz lógica del clúster (LIF) que se conecta al switch del clúster C1 para el nodo n1.
- n1_clus2 es la primera LIF del clúster que se conecta al switch de clúster C2 del nodo n1.
- n2_clus1 es la primera LIF de clúster que se conecta al switch de clúster C1 para el nodo n2.
- n2_clus2 es la segunda LIF del clúster que se conecta al switch de clúster C2 del nodo n2.
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la "[Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®](#)" página.



Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Paso 1: Mostrar y migrar puertos físicos y lógicos

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

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

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



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

2. Determine el estado administrativo u operativo de cada interfaz de clúster:

- a. Mostrar los atributos del puerto de red:

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

Muestra el ejemplo

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
e4e         Cluster      Cluster      up    9000 auto/40000 -
-
Node: n2

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
e4e         Cluster      Cluster      up    9000 auto/40000 -
4 entries were displayed.
```

- b. Muestra información sobre las interfaces lógicas y sus nodos principales designados:

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

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver  Interface  Admin/Oper  Address/Mask  Node
Port    Home
-----
Cluster
e4a      n1_clus1    up/up      10.10.0.1/24  n1
true
e4e      n1_clus2    up/up      10.10.0.2/24  n1
true
e4a      n2_clus1    up/up      10.10.0.3/24  n2
true
e4e      n2_clus2    up/up      10.10.0.4/24  n2
true

4 entries were displayed.
```

- c. Compruebe que la detección de clústeres sin switch esté habilitada mediante el comando de privilegio avanzado:

```
network options detect-switchless-cluster show`
```

Muestra el ejemplo

El resultado en el ejemplo siguiente muestra que la detección de clústeres sin switch está habilitada:

```
cluster::*> network options detect-switchless-cluster show
Enable Switchless Cluster Detection: true
```

3. Verifique que los RCF e imagen adecuados estén instalados en los nuevos conmutadores 3232C y realice las personalizaciones necesarias del sitio, como agregar usuarios, contraseñas y direcciones de red.

Debe preparar ambos switches en este momento. Si necesita actualizar el software RCF e Image, debe seguir estos pasos:

- a. Vaya a la página *Cisco Ethernet Switches* del sitio de soporte de NetApp.

["Switches Ethernet de Cisco"](#)

- b. Anote el conmutador y las versiones de software necesarias en la tabla de esa página.

- c. Descargue la versión adecuada de RCF.
- d. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.
- e. Descargue la versión adecuada del software Image.

["Página de descarga del archivo de configuración de referencia del switch de red de Cisco Cluster y Management"](#)

4. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.
5. En los switches Nexus 3232C C1 y C2, deshabilite todos los puertos C1 y C2 que están orientados al nodo, pero no deshabilite los puertos ISL e1/31-32.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo, se muestran los puertos 1 a 30 deshabilitados en los switches del clúster Nexus 3232C C1 y C2 utilizando una configuración compatible con RCF
NX3232_RCF_v1.0_24p10g_24p100g.txt:

```
C1# copy running-config startup-config
[] 100% Copy complete.
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# shutdown
C1(config-if-range)# exit
C1(config)# exit
C2# copy running-config startup-config
[] 100% Copy complete.
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
```

6. Conecte los puertos 1/31 y 1/32 de C1 a los mismos puertos de C2 utilizando el cableado compatible.
7. Compruebe que los puertos ISL están operativos en C1 y C2:

```
show port-channel summary
```

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

El siguiente ejemplo muestra Cisco `show port-channel summary` Comando que se utiliza para verificar que los puertos ISL están operativos en C1 y C2:

```
C1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
      Port-
Group Channel          Type   Protocol  Member Ports
-----
-----
1      Po1 (SU)         Eth    LACP      Eth1/31 (P)  Eth1/32 (P)

C2# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      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)
```

8. Muestra la lista de dispositivos vecinos en el conmutador.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo se muestra el comando Cisco `show cdp neighbors` se utiliza para mostrar los dispositivos vecinos en el conmutador:

```
C1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C2                  Eth1/31        174    R S I s          N3K-C3232C
Eth1/31
C2                  Eth1/32        174    R S I s          N3K-C3232C
Eth1/32
Total entries displayed: 2
C2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute
Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C1                  Eth1/31        178    R S I s          N3K-C3232C
Eth1/31
C1                  Eth1/32        178    R S I s          N3K-C3232C
Eth1/32
Total entries displayed: 2
```

9. Muestre la conectividad de puerto del clúster en cada nodo:

```
network device-discovery show
```


Muestra el ejemplo

En el siguiente ejemplo se muestra la conectividad de puerto de clúster mostrada para una configuración de clúster de dos nodos sin switch:

```
cluster::*> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform
n1	/cdp			
	e4a	n2	e4a	FAS9000
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	n1	e4a	FAS9000
	e4e	n1	e4e	FAS9000

10. Migre los LIF n1_clus1 y n2_clus1 a los puertos físicos de sus nodos de destino:

```
network interface migrate -vserver vservice-name -lif lif-name source-node  
source-node-name -destination-port destination-port-name
```

Muestra el ejemplo

Debe ejecutar el comando para cada nodo local tal y como se muestra en el ejemplo siguiente:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus1  
-source-node n1  
-destination-node n1 -destination-port e4e  
cluster::*> network interface migrate -vserver cluster -lif n2_clus1  
-source-node n2  
-destination-node n2 -destination-port e4e
```

Paso 2: Apague las LIF reasignadas y desconecte los cables

1. Compruebe que las interfaces del clúster han migrado correctamente:

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

Muestra el ejemplo

En el siguiente ejemplo, se muestra el estado "is Home" de las LIF n1_clus1 y n2_clus1 se ha convertido en "false" una vez completada la migración:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4e      false
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4e      false
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

2. Apague los puertos del clúster de las LIF n1_clus1 y n2_clus1, que se migraron en el paso 9:

```
network port modify -node node-name -port port-name -up-admin false
```

Muestra el ejemplo

Debe ejecutar el comando para cada puerto tal y como se muestra en el ejemplo siguiente:

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

3. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::*> cluster ping-cluster -node n1

Host is n1 Getting addresses from network interface table...
Cluster n1_clus1 n1          e4a      10.10.0.1
Cluster n1_clus2 n1          e4e      10.10.0.2
Cluster n2_clus1 n2          e4a      10.10.0.3
Cluster n2_clus2 n2          e4e      10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
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 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s) RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

4. Desconecte el cable del e4a del nodo n1.

Puede consultar la configuración en ejecución y conectar el primer puerto de 40 GbE del switch C1 (puerto 1/7 en este ejemplo) a e4a en la n1 utilizando el cableado compatible con los switches Nexus 3232C.

Paso 3: Habilite los puertos del clúster

1. Desconecte el cable del e4a del nodo n2.

Puede consultar la configuración en ejecución y conectar e4a al siguiente puerto 40 GbE disponible en C1, puerto 1/8, utilizando el cableado compatible.

2. Habilite todos los puertos orientados al nodo en C1.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

En el siguiente ejemplo se muestran los puertos 1 a 30 habilitados en los switches del clúster Nexus 3232C C1 y C2 que utilizan la configuración admitida en RCF
NX3232_RCF_v1.0_24p10g_26p100g.txt:

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

3. Active el primer puerto del clúster, e4a, en cada nodo:

```
network port modify -node node-name -port port-name -up-admin true
```

Muestra el ejemplo

```
cluster::*> network port modify -node n1 -port e4a -up-admin true
cluster::*> network port modify -node n2 -port e4a -up-admin true
```

4. Compruebe que los clústeres estén en ambos nodos:

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

Muestra el ejemplo

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper Status
Status
-----
-----
e4a       Cluster      Cluster      up    9000 auto/40000 -
e4e       Cluster      Cluster      up    9000 auto/40000 -
-

Node: n2

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper Status
Status
-----
-----
e4a       Cluster      Cluster      up    9000 auto/40000 -
e4e       Cluster      Cluster      up    9000 auto/40000 -

4 entries were displayed.
```

5. Para cada nodo, revierte todos los LIF de interconexión de clúster migrados:

```
network interface revert -vserver cluster -lif lif-name
```

Muestra el ejemplo

Debe revertir cada LIF a su puerto de inicio de forma individual, como se muestra en el ejemplo siguiente:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus1
```

6. Compruebe que todas las LIF se han revertido a sus puertos principales:

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

La Is Home la columna debe mostrar un valor de true para todos los puertos enumerados en la Current Port columna. Si el valor mostrado es false, el puerto no se ha revertido.

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4a true n1_clus1 up/up 10.10.0.1/24 n1
e4e true n1_clus2 up/up 10.10.0.2/24 n1
e4a true n2_clus1 up/up 10.10.0.3/24 n2
e4e true n2_clus2 up/up 10.10.0.4/24 n2
4 entries were displayed.
```

Paso 4: Habilite las LIF reasignadas

1. Muestre la conectividad de puerto del clúster en cada nodo:

```
network device-discovery show
```

Muestra el ejemplo

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	n1	e4e	FAS9000

2. Migre clus2 al puerto e4a de la consola de cada nodo:

```
network interface migrate cluster -lif lif-name -source-node source-node-name  
-destination-node destination-node-name -destination-port destination-port-name
```

Muestra el ejemplo

Debe migrar cada LIF a su puerto de inicio de forma individual, como se muestra en el ejemplo siguiente:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus2  
-source-node n1  
-destination-node n1 -destination-port e4a  
cluster::*> network interface migrate -vserver cluster -lif n2_clus2  
-source-node n2  
-destination-node n2 -destination-port e4a
```

3. Apague los puertos de clúster clus2 LIF en ambos nodos:

```
network port modify
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos especificados que se están estableciendo en false, apagando los puertos en ambos nodos:

```
cluster::*> network port modify -node n1 -port e4e -up-admin false  
cluster::*> network port modify -node n2 -port e4e -up-admin false
```

4. Compruebe el estado de LIF del clúster:

```
network interface show
```

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4a      false
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4a      false
4 entries were displayed.
```

5. Desconecte el cable del e4e en el nodo n1.

Puede consultar la configuración en ejecución y conectar el primer puerto de 40 GbE del switch C2 (puerto 1/7 en este ejemplo) a e4e en el nodo n1, utilizando el cableado adecuado para el modelo de switch Nexus 3232C.

6. Desconecte el cable del e4e en el nodo n2.

Puede consultar la configuración en ejecución y conectar e4e al siguiente puerto de 40 GbE disponible en C2, puerto 1/8, utilizando el cableado adecuado para el modelo de switch Nexus 3232C.

7. Habilite todos los puertos orientados al nodo en C2.

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos 1 a 30 activados en los switches de clúster C1 y C2 de Nexus 3132Q-V. mediante una configuración compatible con RCF

NX3232C_RCF_v1.0_24p10g_26p100g.txt:

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

8. Active el segundo puerto del clúster, e4e, en cada nodo:

```
network port modify
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el segundo puerto e4e del clúster que se está poniendo en marcha en cada nodo:

```
cluster::*> network port modify -node n1 -port e4e -up-admin true
cluster::*> *network port modify -node n2 -port e4e -up-admin true*s
```

9. Para cada nodo, revierte todos los LIF de interconexión de clúster migrados: `network interface revert`

Muestra el ejemplo

En el ejemplo siguiente se muestran los LIF migrados que se han revertido a sus puertos principales.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

10. Verifique que todos los puertos de interconexión de clúster ahora se reviertan a sus puertos raíz:

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

La `Is Home` la columna debe mostrar un valor de `true` para todos los puertos enumerados en la `Current Port` columna. Si el valor mostrado es `false`, el puerto no se ha revertido.

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
e4a      true      n1_clus1      up/up      10.10.0.1/24      n1
e4e      true      n1_clus2      up/up      10.10.0.2/24      n1
e4a      true      n2_clus1      up/up      10.10.0.3/24      n2
e4e      true      n2_clus2      up/up      10.10.0.4/24      n2
4 entries were displayed.
```

11. Compruebe que todos los puertos de interconexión del clúster se encuentren en la up provincia:

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

12. Muestre los números de puerto del switch del clúster a través de los cuales cada puerto del clúster está conectado a cada nodo: `network device-discovery show`

Muestra el ejemplo

```
cluster::*> network device-discovery show
      Local   Discovered
Node      Port   Device      Interface      Platform
-----
n1      /cdp
e4a      C1      Ethernet1/7      N3K-C3232C
e4e      C2      Ethernet1/7      N3K-C3232C
n2      /cdp
e4a      C1      Ethernet1/8      N3K-C3232C
e4e      C2      Ethernet1/8      N3K-C3232C
```

13. Mostrar switches de clúster detectados y supervisados:

```
system cluster-switch show
```

Muestra el ejemplo

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3232CV Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP	cluster-network	10.10.1.101
C2 NX3232CV Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP	cluster-network	10.10.1.102

2 entries were displayed.

14. Compruebe que la detección del clúster sin switches ha cambiado la opción de clúster sin switches a deshabilitado:

```
network options switchless-cluster show
```

15. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

```
cluster::*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1_clus1 n1          e4a    10.10.0.1
Cluster n1_clus2 n1          e4e    10.10.0.2
Cluster n2_clus1 n2          e4a    10.10.0.3
Cluster n2_clus2 n2          e4e    10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
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 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s) RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

16. Habilite la función de recogida de registro de supervisión del estado del switch para recopilar archivos de registro relacionados con el switch:

```
system cluster-switch log setup-password
```

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

Muestra el ejemplo

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

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

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

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

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

Enabling cluster switch log collection.

cluster::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

17. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

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

Sustituya los interruptores

Sustituya un switch de clúster Cisco Nexus 3232C

Siga estos pasos para sustituir un switch Cisco Nexus 3232C defectuoso en un clúster. Este procedimiento no es disruptivo.

Revise los requisitos

Lo que necesitará

Asegúrese de que la configuración de clúster y red existente tenga las siguientes características:

- La infraestructura del clúster Nexus 3232C es redundante y totalmente funcional en ambos switches.

La página Cisco Ethernet Switches tiene las versiones más recientes de RCF y NX-OS en sus switches.

- Todos los puertos del clúster deben estar en el estado **up**.
- Debe haber conectividad de gestión en ambos switches.
- Todas las interfaces lógicas de clúster (LIF) están en el estado **up** y no se migran.

El switch Cisco Nexus 3232C de sustitución tiene las siguientes características:

- La conectividad de la red de gestión es funcional.
- El acceso de la consola al interruptor de sustitución está en su lugar.
- La imagen apropiada del sistema operativo RCF y NX-OS se carga en el conmutador.
- Se ha completado la personalización inicial del conmutador.

Si quiere más información

Consulte lo siguiente:

- ["Página de descripción de Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Sustituya el interruptor

Acerca de esta tarea

Este procedimiento de sustitución describe la siguiente situación:

- Al principio, el clúster tiene cuatro nodos conectados a dos switches de clúster Nexus 3232C, CL1 y CL2.
- Tiene previsto sustituir el conmutador de clúster CL2 por C2 (pasos del 1 al 21):
 - En cada nodo, migra las LIF de clúster conectadas al switch del clúster CL2 a los puertos del clúster conectados al switch del clúster CL1.
 - Desconecte el cableado de todos los puertos del switch del clúster CL2 y vuelva a conectar el cableado a los mismos puertos del switch del clúster de reemplazo C2.
 - Revierte los LIF de clúster migrados en cada nodo.

Acerca de los ejemplos

Este procedimiento de sustitución sustituye al segundo switch de clúster Nexus 3232C CL2 por el nuevo switch 3232C C2.

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

- Los cuatro nodos son n1, n2, n3 y n4.
- n1_clus1 es la primera interfaz lógica del clúster (LIF) conectada al switch del clúster C1 para el nodo n1.
- n1_clus2 es la primera LIF del clúster conectada al switch de clúster CL2 o C2 para el nodo n1.
- n1_clus3 es la segunda LIF conectada al switch de clúster C2 para el nodo n1.-
- n1_clus4 es la segunda LIF conectada al switch de clúster CL1, para el nodo n1.

El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) página.

Los ejemplos de este procedimiento de sustitución utilizan cuatro nodos. Dos de estos nodos utilizan cuatro puertos de interconexión de clúster de 10 GB: E0a, e0b, e0c y e0d. Los otros dos nodos utilizan dos puertos de interconexión de clúster de 40 GB: e4a y e4e. Consulte ["Hardware Universe"](#) para verificar los puertos de clúster correctos para su plataforma.

Paso 1: Mostrar y migrar los puertos del clúster al switch

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

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

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



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

2. Muestra información sobre los dispositivos de la configuración:

```
network device-discovery show
```

Muestra el ejemplo

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform

n1	/cdp			
	e0a	CL1	Ethernet1/1/1	N3K-C3232C
	e0b	CL2	Ethernet1/1/1	N3K-C3232C
	e0c	CL2	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3232C
	e0b	CL2	Ethernet1/1/3	N3K-C3232C
	e0c	CL2	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3232C
	e4e	CL2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	CL1	Ethernet1/8	N3K-C3232C
	e4e	CL2	Ethernet1/8	N3K-C3232C

3. Determinar el estado administrativo u operativo de cada interfaz de clúster.

a. Mostrar los atributos del puerto de red:

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



```

cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Speed (Mbps)

Health  Health
Port    IPspace  Broadcast Domain Link MTU  Admin/Oper
Status  Status

-----
-----
e0a      Cluster  Cluster          up    9000  auto/10000 -
e0b      Cluster  Cluster          up    9000  auto/10000 -
e0c      Cluster  Cluster          up    9000  auto/10000 -
e0d      Cluster  Cluster          up    9000  auto/10000 -
-

Node: n2

Ignore

Speed (Mbps)

Health  Health
Port    IPspace  Broadcast Domain Link MTU  Admin/Oper
Status  Status

-----
-----
e0a      Cluster  Cluster          up    9000  auto/10000 -
e0b      Cluster  Cluster          up    9000  auto/10000 -
e0c      Cluster  Cluster          up    9000  auto/10000 -
e0d      Cluster  Cluster          up    9000  auto/10000 -
-

Node: n3

Ignore

Speed (Mbps)

Health  Health
Port    IPspace  Broadcast Domain Link MTU  Admin/Oper
Status  Status

-----
-----
e4a      Cluster  Cluster          up    9000  auto/40000 -
-
e4e      Cluster  Cluster          up    9000  auto/40000 -

```

```

-

Node: n4

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
e4e         Cluster      Cluster      up    9000 auto/40000 -

```

b. Mostrar información acerca de las interfaces lógicas (LIF):

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

Muestra el ejemplo

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

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

Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e0a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e0e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e0a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e0e	true			

c. Muestre los switches del clúster detectados:

```
system cluster-switch show
```

Muestra el ejemplo

En el siguiente ejemplo de resultado se muestran los switches de clúster:

```
cluster::> system cluster-switch show
```

Switch	Type	Address
CL1	cluster-network	10.10.1.101
NX3232C		
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
CL2	cluster-network	10.10.1.102
NX3232C		
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		

4. Compruebe que el RCF y la imagen adecuados están instalados en el nuevo switch Nexus 3232C y realice las personalizaciones necesarias del sitio.
 - a. Vaya al sitio de soporte de NetApp.
["mysupport.netapp.com"](https://mysupport.netapp.com)
 - b. Vaya a la página **Cisco Ethernet Switches** y anote las versiones de software necesarias en la tabla.
["Switches Ethernet de Cisco"](#)
 - c. Descargue la versión adecuada del RCF.
 - d. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, vaya a la página **Descargar**.
 - e. Descargue la versión correcta del software Image desde la página *Descarga del archivo de configuración de referencia del conmutador de red de administración y clúster Cisco®.

["Descarga del archivo de configuración de referencia del conmutador de red de administración y clúster Cisco®"](#)

5. Migre las LIF del clúster a los puertos del nodo físico conectados al switch de reemplazo C2:

```
network interface migrate -vserver vserver-name -lif lif-name -source-node
node-name -destination-node node-name -destination-port port-name
```

Muestra el ejemplo

Debe migrar todas las LIF del clúster individualmente, como se muestra en el ejemplo siguiente:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -destination-
node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -destination-
node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -destination-
node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -destination-
node n2 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2
-source-node n3 -destination-
node n3 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2
-source-node n4 -destination-
node n4 -destination-port e4a
```

6. Compruebe el estado de los puertos del clúster y sus designaciones principales:

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

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
e0a          n1_clus1    up/up      10.10.0.1/24      n1
true
e0a          n1_clus2    up/up      10.10.0.2/24      n1
false
e0d          n1_clus3    up/up      10.10.0.3/24      n1
false
e0d          n1_clus4    up/up      10.10.0.4/24      n1
true
e0a          n2_clus1    up/up      10.10.0.5/24      n2
true
e0a          n2_clus2    up/up      10.10.0.6/24      n2
false
e0d          n2_clus3    up/up      10.10.0.7/24      n2
false
e0d          n2_clus4    up/up      10.10.0.8/24      n2
true
e4a          n3_clus1    up/up      10.10.0.9/24      n3
true
e4a          n3_clus2    up/up      10.10.0.10/24     n3
false
e4a          n4_clus1    up/up      10.10.0.11/24     n4
true
e4a          n4_clus2    up/up      10.10.0.12/24     n4
false
```

7. Apague los puertos de interconexión de clúster que están conectados físicamente al switch CL2 original:

```
network port modify -node node-name -port port-name -up-admin false
```

Muestra el ejemplo

En el siguiente ejemplo se muestran los puertos de interconexión de clúster se apagan en todos los nodos:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1_clus1 n1          e0a      10.10.0.1
Cluster n1_clus2 n1          e0b      10.10.0.2
Cluster n1_clus3 n1          e0c      10.10.0.3
Cluster n1_clus4 n1          e0d      10.10.0.4
Cluster n2_clus1 n2          e0a      10.10.0.5
Cluster n2_clus2 n2          e0b      10.10.0.6
Cluster n2_clus3 n2          e0c      10.10.0.7
Cluster n2_clus4 n2          e0d      10.10.0.8
Cluster n3_clus1 n4          e0a      10.10.0.9
Cluster n3_clus2 n3          e0e      10.10.0.10
Cluster n4_clus1 n4          e0a      10.10.0.11
Cluster n4_clus2 n4          e0e      10.10.0.12
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11
10.10.0.12 Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s) .....
Detected 9000 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.1 to Remote 10.10.0.9
  Local 10.10.0.1 to Remote 10.10.0.10
  Local 10.10.0.1 to Remote 10.10.0.11
  Local 10.10.0.1 to Remote 10.10.0.12
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.9
  Local 10.10.0.2 to Remote 10.10.0.10
  Local 10.10.0.2 to Remote 10.10.0.11
  Local 10.10.0.2 to Remote 10.10.0.12
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
```



```
Local 10.10.0.3 to Remote 10.10.0.9
Local 10.10.0.3 to Remote 10.10.0.10
Local 10.10.0.3 to Remote 10.10.0.11
Local 10.10.0.3 to Remote 10.10.0.12
Local 10.10.0.4 to Remote 10.10.0.5
Local 10.10.0.4 to Remote 10.10.0.6
Local 10.10.0.4 to Remote 10.10.0.7
Local 10.10.0.4 to Remote 10.10.0.8
Local 10.10.0.4 to Remote 10.10.0.9
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s) RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

Paso 2: Migrar ISL al switch CL1 y C2

1. Apague los puertos 1/31 y 1/32 en el conmutador de grupo CL1.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

```
(CL1)# configure
(CL1) (Config)# interface e1/31-32
(CL1) (config-if-range)# shutdown
(CL1) (config-if-range)# exit
(CL1) (Config)# exit
(CL1)#
```

2. Retire todos los cables conectados al switch del clúster CL2 y vuelva a conectarlos al conmutador C2 de sustitución para todos los nodos.
3. Retire los cables de enlace entre switches (ISL) de los puertos e1/31 y e1/32 en el switch del clúster CL2 y vuelva a conectarlos a los mismos puertos en el switch de reemplazo C2.
4. Conecte los puertos ISL 1/31 y 1/32 en el switch de clúster CL1.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1) (config-if-range) # no shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

5. Verifique que los ISL estén activos en CL1.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Los puertos eth1/31 y eth1/32 deben indicar (P), Lo que significa que los puertos ISL están activos en el canal de puerto:

Muestra el ejemplo

```
CL1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      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)
```

6. Compruebe que los ISL estén activos en el switch del clúster C2.

Para obtener más información acerca de los comandos de Cisco, consulte las guías que se enumeran en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Muestra el ejemplo

Los puertos eth1/31 y eth1/32 deben indicar (P), lo cual significa que ambos puertos ISL están activos en el puerto-canal.

```
C2# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      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)
```

7. En todos los nodos, active todos los puertos de interconexión del clúster conectados al switch de reemplazo C2:

```
network port modify -node node-name -port port-name -up-admin true
```

Muestra el ejemplo

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
cluster::*> network port modify -node n3 -port e4e -up-admin true
cluster::*> network port modify -node n4 -port e4e -up-admin true
```

Paso 3: Revierte todas las LIF a los puertos asignados originalmente

1. Revierte todos los LIF de interconexión de clúster migrados en todos los nodos:

```
network interface revert -vserver cluster -lif lif-name
```

Muestra el ejemplo

Debe revertir todas las LIF de interconexión del clúster individualmente, tal y como se muestra en el ejemplo siguiente:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2
cluster::*> network interface revert -vserver cluster -lif n1_clus3
cluster::*> network interface revert -vserver cluster -lif n2_clus2
cluster::*> network interface revert -vserver cluster -lif n2_clus3
Cluster::*> network interface revert -vserver cluster -lif n3_clus2
Cluster::*> network interface revert -vserver cluster -lif n4_clus2
```

2. Compruebe que los puertos de interconexión de clúster ahora se han revertido a su origen:

```
network interface show
```

Muestra el ejemplo

El siguiente ejemplo muestra que todas las LIF se han revertido correctamente porque los puertos enumerados en Current Port la columna tiene el estado de true en la Is Home columna. Si un puerto tiene un valor de false, El LIF no se ha revertido.

```
cluster::*> network interface show -role cluster
(network interface show)
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

3. Compruebe que los puertos del clúster están conectados:

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

Muestra el ejemplo

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

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

```
Speed(Mbps) Health
```

```
Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
```

```
-----
```

```
e0a      Cluster      Cluster      up    9000  auto/10000  -
e0b      Cluster      Cluster      up    9000  auto/10000  -
e0c      Cluster      Cluster      up    9000  auto/10000  -
e0d      Cluster      Cluster      up    9000  auto/10000  -
-
```

```
Node: n2
```

```
Ignore
```

```
Speed(Mbps) Health
```

```
Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
```

```
-----
```

```
e0a      Cluster      Cluster      up    9000  auto/10000  -
e0b      Cluster      Cluster      up    9000  auto/10000  -
e0c      Cluster      Cluster      up    9000  auto/10000  -
e0d      Cluster      Cluster      up    9000  auto/10000  -
-
```

```
Node: n3
```

```
Ignore
```

```
Speed(Mbps) Health
```

```
Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
```

```
-----
```

```
e4a      Cluster      Cluster      up    9000  auto/40000  -
e4e      Cluster      Cluster      up    9000  auto/40000  -
-
```

```
Node: n4
```

Ignore

Speed (Mbps) Health

Health

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
------	---------	-----------	--------	------	-----	------------	--------

e4a	Cluster	Cluster		up	9000	auto/40000	-
-----	---------	---------	--	----	------	------------	---

e4e	Cluster	Cluster		up	9000	auto/40000	-
-----	---------	---------	--	----	------	------------	---

-							
---	--	--	--	--	--	--	--

4. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el nodo n1 con alas y el estado RPC indicado posteriormente:

```
cluster::*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1_clus1 n1          e0a      10.10.0.1
Cluster n1_clus2 n1          e0b      10.10.0.2
Cluster n1_clus3 n1          e0c      10.10.0.3
Cluster n1_clus4 n1          e0d      10.10.0.4
Cluster n2_clus1 n2          e0a      10.10.0.5
Cluster n2_clus2 n2          e0b      10.10.0.6
Cluster n2_clus3 n2          e0c      10.10.0.7
Cluster n2_clus4 n2          e0d      10.10.0.8
Cluster n3_clus1 n3          e0a      10.10.0.9
Cluster n3_clus2 n3          e0e      10.10.0.10
Cluster n4_clus1 n4          e0a      10.10.0.11
Cluster n4_clus2 n4          e0e      10.10.0.12
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s) .....
Detected 1500 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.1 to Remote 10.10.0.9
  Local 10.10.0.1 to Remote 10.10.0.10
  Local 10.10.0.1 to Remote 10.10.0.11
  Local 10.10.0.1 to Remote 10.10.0.12
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.9
  Local 10.10.0.2 to Remote 10.10.0.10
  Local 10.10.0.2 to Remote 10.10.0.11
  Local 10.10.0.2 to Remote 10.10.0.12
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
```



```
Local 10.10.0.3 to Remote 10.10.0.9
Local 10.10.0.3 to Remote 10.10.0.10
Local 10.10.0.3 to Remote 10.10.0.11
Local 10.10.0.3 to Remote 10.10.0.12
Local 10.10.0.4 to Remote 10.10.0.5
Local 10.10.0.4 to Remote 10.10.0.6
Local 10.10.0.4 to Remote 10.10.0.7
Local 10.10.0.4 to Remote 10.10.0.8
Local 10.10.0.4 to Remote 10.10.0.9
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s) RPC status:
8 paths up, 0 paths down (tcp check)
8  paths up, 0 paths down (udp check)
```

Paso 4: Verificar que todos los puertos y LIF se han migrado correctamente

1. Para mostrar la información sobre los dispositivos de la configuración, introduzca los siguientes comandos:

Puede ejecutar los siguientes comandos en cualquier orden:

- ° network device-discovery show
- ° network port show -role cluster
- ° network interface show -role cluster
- ° system cluster-switch show

Muestra el ejemplo

```
cluster::> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

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

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status

e0a	Cluster	Cluster		up	9000	auto/10000	-
e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c	Cluster	Cluster		up	9000	auto/10000	-
e0d	Cluster	Cluster		up	9000	auto/10000	-

```
Node: n2
```

```
Ignore
```

						Speed(Mbps)	Health
Health							

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status

e0a	Cluster	Cluster		up	9000	auto/10000	-
e0b	Cluster	Cluster		up	9000	auto/10000	-
e0c	Cluster	Cluster		up	9000	auto/10000	-
e0d	Cluster	Cluster		up	9000	auto/10000	-

Node: n3

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status

e4a	Cluster	Cluster		up	9000	auto/40000	-
e4e	Cluster	Cluster		up	9000	auto/40000	-

Node: n4

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status

e4a	Cluster	Cluster		up	9000	auto/40000	-
e4e	Cluster	Cluster		up	9000	auto/40000	-

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

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

Cluster					
	nm1_clus1	up/up	10.10.0.1/24	n1	
e0a	true				
	n1_clus2	up/up	10.10.0.2/24	n1	
e0b	true				

	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

cluster::*> **system cluster-switch show**

Switch	Type	Address
Model		
-----	-----	-----
CL1	cluster-network	10.10.1.101
NX3232C		
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
CL2	cluster-network	10.10.1.102
NX3232C		
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2	cluster-network	10.10.1.103
NX3232C		
Serial Number: FOX000003		

```
Is Monitored: true
```

```
Reason: None
```

```
Software Version: Cisco Nexus Operating System (NX-OS)
```

```
Software, Version 7.0(3)I6(1)
```

```
Version Source: CDP 3 entries were displayed.
```

2. Elimine el interruptor del grupo de instrumentos sustituido CL2 si no se ha quitado automáticamente:

```
system cluster-switch delete -device cluster-switch-name
```

3. Compruebe que se supervisan los switches de clúster adecuados:

```
system cluster-switch show
```

Muestra el ejemplo

En el siguiente ejemplo se muestran los switches de clúster se supervisan porque Is Monitored el estado es true.

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3232C	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		

4. Habilite la función de recogida de registro de supervisión del estado del switch para recopilar archivos de registro relacionados con el switch:

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

Muestra el ejemplo

```
cluster::*> system cluster-switch log setup-password  
Enter the switch name: <return>  
The switch name entered is not recognized.  
Choose from the following list:  
CL1  
C2  
  
cluster::*> system cluster-switch log setup-password  
  
Enter the switch name: CL1  
RSA key fingerprint is  
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc  
Do you want to continue? {y|n}::[n] y  
  
Enter the password: <enter switch password>  
Enter the password again: <enter switch password>  
  
cluster::*> system cluster-switch log setup-password  
  
Enter the switch name: C2  
RSA key fingerprint is  
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1  
Do you want to continue? {y|n}: [n] y  
  
Enter the password: <enter switch password>  
Enter the password again: <enter switch password>  
  
cluster::*> system cluster-switch log enable-collection  
  
Do you want to enable cluster log collection for all nodes in the  
cluster?  
{y|n}: [n] y  
  
Enabling cluster switch log collection.  
  
cluster::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

5. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

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

Sustituya un switch de almacenamiento Cisco Nexus 3232C

Siga estos pasos para sustituir un switch de almacenamiento Cisco Nexus 3232C defectuoso. Este procedimiento no es disruptivo.

Revise los requisitos

La configuración de red existente debe tener las siguientes características:

- La página Cisco Ethernet Switches tiene las versiones más recientes de RCF y NX-OS en sus switches.
- Debe haber conectividad de gestión en ambos switches.



Asegúrese de que se han completado todos los pasos de solución de problemas para confirmar que es necesario sustituir el interruptor.

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

- La conectividad de la red de gestión debe ser funcional.
- El acceso de la consola al interruptor de sustitución debe estar en su lugar.
- Se deben cargar en el conmutador las imágenes del sistema operativo RCF y NX-OS adecuadas.
- Se debe completar la personalización inicial del conmutador.

Sustituya el interruptor

Este procedimiento reemplaza al segundo switch de almacenamiento Nexus 3232C S2 con el nuevo switch 3232C NS2. Los dos nodos son 1 y 2.

Paso 1: Confirmar que el interruptor que se va a sustituir es S2

1. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport: `system node autosupport invoke -node * -type all - message MAINT=xh`

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



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

2. Compruebe el estado de los puertos del nodo de almacenamiento para asegurarse de que exista conexión al switch de almacenamiento S1:

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

Muestra el ejemplo

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

Node	Port	Type	Mode	Speed	State	Status	VLAN
				(Gb/s)			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 interruptor de almacenamiento S1 esté disponible:

```
network device-discovery show
```


Muestra el ejemplo

```
storage::*> network device-discovery show
```

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

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

4. Ejecute el `show lldp neighbors` comando en el switch de trabajo para confirmar que puede ver tanto los nodos como todas las bandejas:

```
show lldp neighbors
```

Muestra el 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: Configure el cableado

1. Compruebe los puertos de las bandejas del sistema de almacenamiento:

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

Muestra el 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 sustitución NS2.

Paso 3: Verifique todas las configuraciones del dispositivo en el conmutador NS2

1. Compruebe el estado de los puertos del nodo de almacenamiento:

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

Muestra el 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
30
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
```

2. Compruebe que ambos conmutadores estén disponibles:

```
network device-discovery show
```

Muestra el ejemplo

```
storage::*> network device-discovery show
```

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

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. Compruebe los puertos de la bandeja en el sistema de almacenamiento:

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

Muestra el 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 ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

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

Sustituya los switches de clúster Cisco Nexus 3232C por conexiones sin switches

Puede migrar desde un clúster con una red de clúster conmutada a uno donde dos nodos están conectados directamente para ONTAP 9.3 y versiones posteriores.

Revise los requisitos

Directrices

Revise las siguientes directrices:

- La migración a una configuración de clúster de dos nodos sin switch es una operación no disruptiva. La mayoría de los sistemas tienen dos puertos de interconexión de clúster dedicados en cada nodo, pero también puede usar este procedimiento para sistemas con un número mayor de puertos de interconexión de clúster dedicados en cada nodo, como cuatro, seis u ocho.
- No se puede usar la función de interconexión de clúster sin switches con más de dos nodos.
- Si tiene un clúster de dos nodos existente que utiliza switches de interconexión de clúster y ejecuta ONTAP 9.3 o una versión posterior, puede reemplazar los switches por conexiones directas de vuelta a atrás entre los nodos.

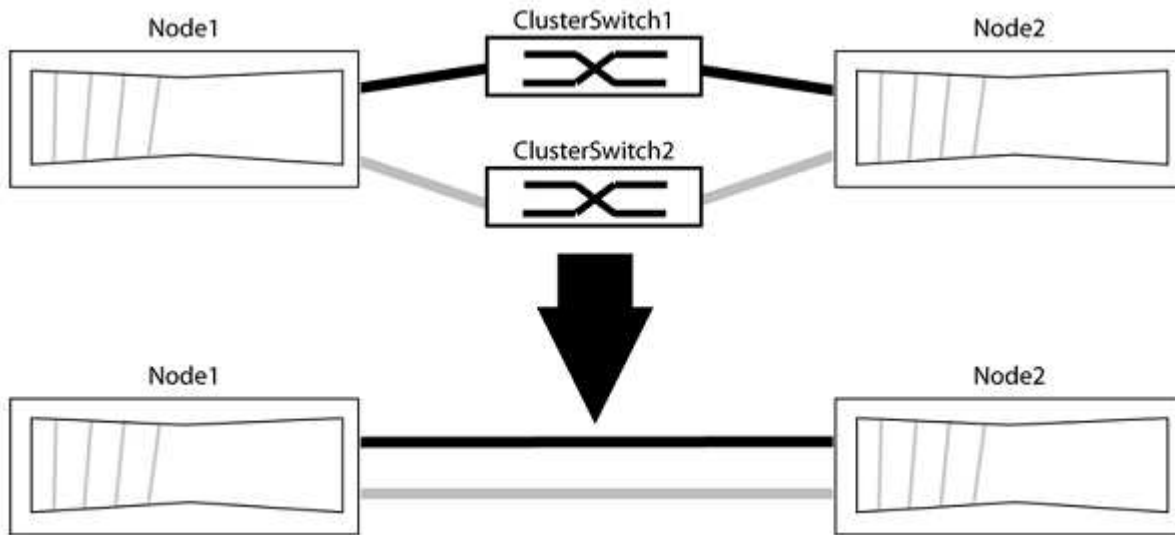
Lo que necesitará

- Un clúster en buen estado que consta de dos nodos conectados por switches de clúster. Los nodos deben ejecutar la misma versión de ONTAP.
- Cada nodo con el número requerido de puertos de clúster dedicados, que proporcionan conexiones redundantes de interconexión de clúster para admitir la configuración de su sistema. Por ejemplo, hay dos puertos redundantes para un sistema con dos puertos de Cluster Interconnect dedicados en cada nodo.

Migrar los switches

Acerca de esta tarea

En el siguiente procedimiento, se quitan los switches de clúster de dos nodos y se reemplaza cada conexión al switch por una conexión directa al nodo compañero.



Acerca de los ejemplos

Los ejemplos del siguiente procedimiento muestran nodos que utilizan «e0a» y «e0b» como puertos del clúster. Sus nodos pueden usar distintos puertos de clúster según varían según el sistema.

Paso 1: Preparación para la migración

1. Cambie el nivel de privilegio a Advanced, introduzca `y` cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado `*>` aparece.

2. ONTAP 9.3 y versiones posteriores admiten la detección automática de clústeres sin switch, que está habilitado de forma predeterminada.

Puede verificar que la detección de clústeres sin switch esté habilitada mediante el comando de privilegio avanzado:

```
network options detect-switchless-cluster show
```

Muestra el ejemplo

El siguiente resultado de ejemplo muestra si la opción está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Si la opción "Activar detección de clústeres sin switch" es `false` Póngase en contacto con el soporte de NetApp.

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

```
system node autosupport invoke -node * -type all -message  
MAINT=<number_of_hours>h
```

donde *h* es la duración del plazo de mantenimiento en horas. El mensaje notifica al soporte técnico de esta tarea de mantenimiento para que estos puedan impedir la creación automática de casos durante la ventana de mantenimiento.

En el ejemplo siguiente, el comando suprime la creación automática de casos durante dos horas:

Muestra el ejemplo

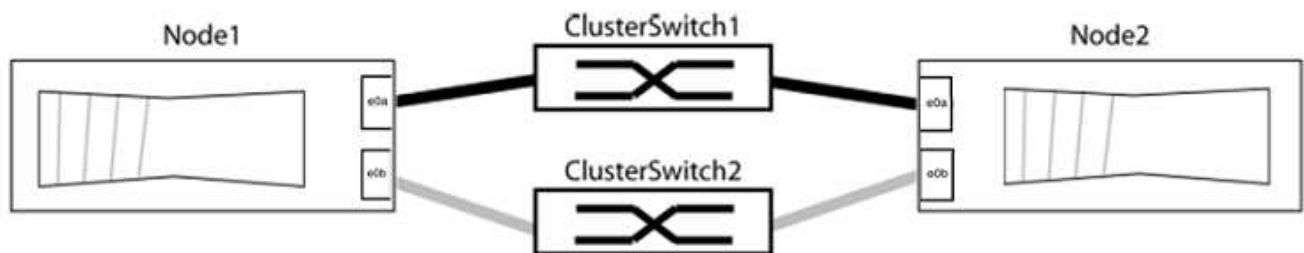
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

Paso 2: Configure los puertos y el cableado

1. Organice los puertos del clúster en cada switch en grupos de modo que los puertos del clúster en group1 vayan a Cluster switch1 y los puertos del cluster en group2 vayan a cluster switch2. Estos grupos son necesarios más adelante en el procedimiento.
2. Identificar los puertos del clúster y verificar el estado y el estado del enlace:

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

En el siguiente ejemplo, en el caso de nodos con puertos de clúster "e0a" y "e0b", un grupo se identifica como "1:e0a" y "2:e0a" y el otro grupo como "1:e0b" y "2:e0b". Sus nodos pueden usar puertos de clúster diferentes porque varían según el sistema.



Compruebe que los puertos tienen un valor de `up` Para la columna "Link" y un valor de `healthy` Para la columna "Estado de salud".

Muestra el ejemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

3. Confirmar que todas las LIF de clúster están en sus puertos raíz.

Compruebe que la columna "es-home" es true Para cada LIF del clúster:

```
network interface show -vserver Cluster -fields is-home
```


Muestra el ejemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-----  -
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Si hay LIF de clúster que no estén en sus puertos raíz, revierte estos LIF a sus puertos principales:

```
network interface revert -vserver Cluster -lif *
```

4. Deshabilite la reversión automática para las LIF del clúster:

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

5. Compruebe que todos los puertos enumerados en el paso anterior están conectados a un conmutador de red:

```
network device-discovery show -port cluster_port
```

La columna “dispositivo detectado” debe ser el nombre del conmutador de clúster al que está conectado el puerto.

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster «e0a» y «e0b» están conectados correctamente a los switches del clúster «cs1» y «cs2».

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e0a    cs1                      0/11       BES-53248
          e0b    cs2                      0/12       BES-53248
node2/cdp
          e0a    cs1                      0/9        BES-53248
          e0b    cs2                      0/9        BES-53248
4 entries were displayed.
```

6. Compruebe la conectividad del clúster:

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

7. Compruebe que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

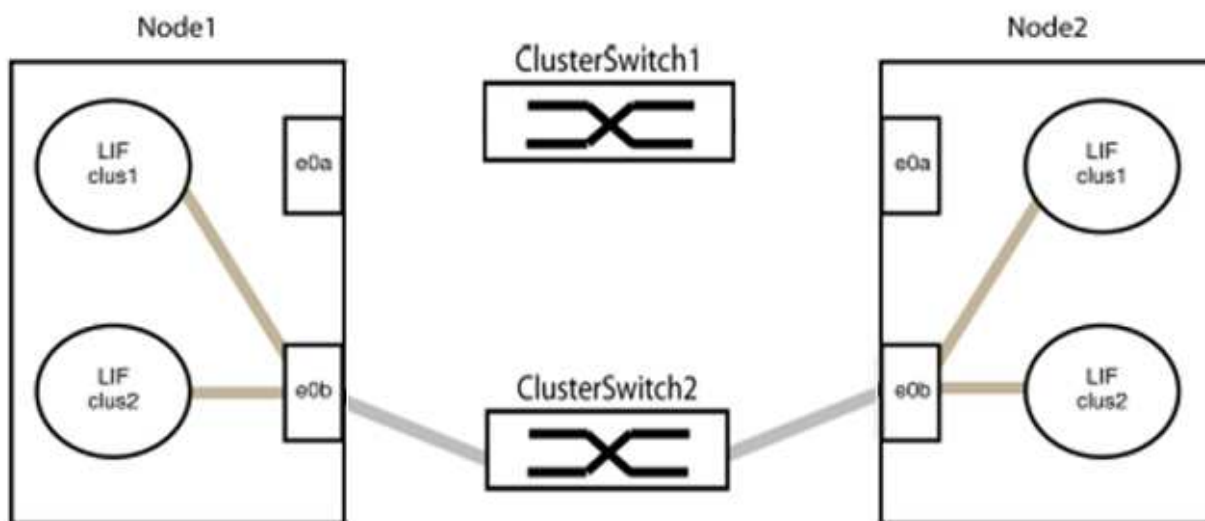
8. Configure la configuración sin switches para los puertos del grupo 1.



Para evitar posibles problemas de red, debe desconectar los puertos del grupo 1 y volver a conectarlos lo antes posible, por ejemplo, **en menos de 20 segundos**.

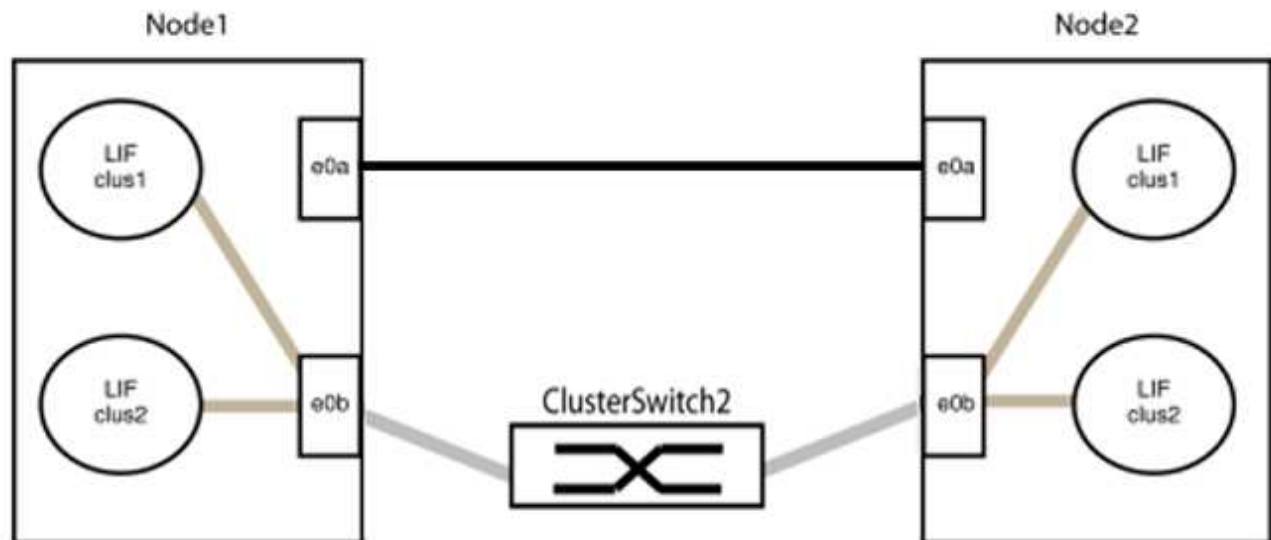
a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

En el ejemplo siguiente, los cables se desconectan del puerto "e0a" en cada nodo, y el tráfico del clúster continúa a través del switch y el puerto "e0b" en cada nodo:



b. Conecte los puertos en group1 de vuelta a espalda.

En el siguiente ejemplo, "e0a" en el nodo 1 está conectado a "e0a" en el nodo 2:



9. La opción de red de clúster sin switch desde la transición `false` para `true`. Esto puede tardar hasta 45 segundos. Confirme que la opción sin switches está establecida en `true`:

```
network options switchless-cluster show
```

En el siguiente ejemplo se muestra que el clúster sin switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

10. Compruebe que la red de clúster no se haya interrumpido:

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



Antes de continuar con el siguiente paso, debe esperar al menos dos minutos para confirmar una conexión de retroceso en funcionamiento en el grupo 1.

11. Configure la configuración sin switches para los puertos del grupo 2.



Para evitar posibles problemas de red, debe desconectar los puertos del grupo 2 y volver a conectarlos lo antes posible, por ejemplo, **en menos de 20 segundos**.

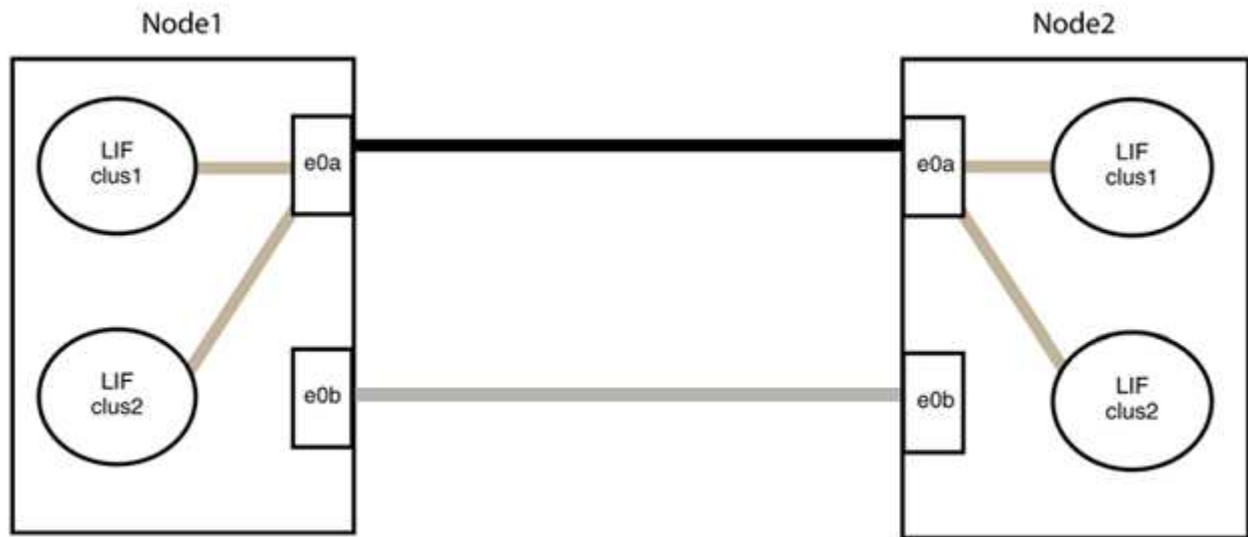
- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

En el ejemplo siguiente, los cables se han desconectado del puerto "e0b" en cada nodo y el tráfico del clúster continúa por la conexión directa entre los puertos "e0a":



b. Conecte los puertos en group2 de vuelta a back.

En el ejemplo siguiente, hay conectado "e0a" en el nodo 1 a "e0a" en el nodo 2 y "e0b" en el nodo 1 está conectado a "e0b" en el nodo 2:



Paso 3: Verificar la configuración

1. Compruebe que los puertos de ambos nodos están conectados correctamente:

```
network device-discovery show -port cluster_port
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster «e0a» y «e0b» están conectados correctamente al puerto correspondiente del partner de clúster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
           e0a    node2                      e0a        AFF-A300
           e0b    node2                      e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                      e0a        AFF-A300
           e0b    node1                      e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Volver a habilitar la reversión automática para las LIF del clúster:

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

3. Compruebe que todas las LIF son Home. Esto puede tardar unos segundos.

```
network interface show -vserver Cluster -lif lif_name
```

Muestra el ejemplo

Los LIF se han revertido si la columna “es de inicio” es true, como se muestra para node1_clus2 y.. node2_clus2 en el siguiente ejemplo:

```
cluster::> network interface show -vserver Cluster -fields curr-  
port,is-home  
vserver  lif                curr-port is-home  
-----  
Cluster  node1_clus1        e0a      true  
Cluster  node1_clus2        e0b      true  
Cluster  node2_clus1        e0a      true  
Cluster  node2_clus2        e0b      true  
4 entries were displayed.
```

Si alguna LIFS de cluster no ha regresado a sus puertos de directorio raíz, revierta manualmente desde el nodo local:

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

4. Compruebe el estado del clúster de los nodos desde la consola del sistema de cualquier nodo:

```
cluster show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra *epsilon* en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true      false  
node2 true    true      false  
2 entries were displayed.
```

5. Confirme la conectividad entre los puertos del clúster:

```
cluster ping-cluster local
```

6. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

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

Para obtener más información, consulte ["Artículo de la base de conocimientos de NetApp 1010449: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#).

7. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

Actualice un switch de almacenamiento de 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.

Revise los requisitos

Lo que necesitará

Asegúrese de que existen las siguientes condiciones antes de actualizar el software NX-OS y los RCF del switch de almacenamiento:

- El conmutador funciona completamente (no debe haber errores en los registros o problemas similares).
- Ha comprobado o establecido las variables de arranque deseadas en el RCF para reflejar las imágenes de arranque deseadas si sólo instala NX-OS y mantiene su versión actual de RCF.

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

- Ha hecho referencia a las guías de software y actualización adecuadas disponibles en la ["Switches Cisco Nexus serie 3000"](#) Para obtener 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 ["Switches Cisco® Ethernet"](#) página.

Sustituya el interruptor

Acerca de los ejemplos

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

- Los nombres de los dos interruptores de almacenamiento son S1 y S2.
- Los nodos son 1 y 2.

Los ejemplos de este procedimiento utilizan dos nodos, uno nodo 1 con dos puertos de almacenamiento y otro nodo 2 con dos puertos de almacenamiento. Consulte ["Hardware Universe"](#) para verificar los puertos de almacenamiento correctos en sus plataformas.



Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario. Los resultados del comando pueden variar en función de las diferentes versiones de ONTAP.

Paso 1: Compruebe el estado de los switches y los puertos

1. Si AutoSupport está habilitado, elimine 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 de esta tarea de mantenimiento para que la creación automática de casos se suprima durante la ventana de mantenimiento.

2. Compruebe que estén disponibles los switches de almacenamiento:

```
system switch ethernet show
```

Muestra el 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. Compruebe que los puertos del nodo estén en buen estado y estén operativos:

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


Muestra el ejemplo

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

VLAN	Port	Type	Mode	Speed (Gb/s)	State	Status
Node 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 en cableado o switch de almacenamiento:

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

Muestra el ejemplo

```
storage::*> system health alert show -instance
```

There are no entries matching your query.

Paso 2: Copie el RCF al conmutador S2 de Cisco

1. Copie el RCF del switch S2 en el bootflash del switch utilizando uno de los siguientes protocolos de transferencia: FTP, HTTP, TFTP, SFTP o SCP.

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

Muestra el ejemplo

El siguiente ejemplo muestra que se está utilizando HTTP para copiar un RCF al bootflash 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 anteriormente al flash de arranque:

```
copy bootflash:
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el archivo RCF Nexus_3232C_RCF_v1.6-Storage.txt Instalación en el interruptor S2:

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

3. Compruebe que el archivo RCF es la versión más reciente correcta:

```
show running-config
```

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

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

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



En el resultado del banner desde la `show banner motd` Debe leer y seguir las instrucciones de la sección **NOTAS IMPORTANTES** para asegurarse de que la configuración y el funcionamiento del interruptor son correctos.

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

4. Después de verificar que las versiones de software y los ajustes del switch son correctos, copie el `running-config` en la `startup-config` Archivo en el interruptor S2.

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

Muestra el ejemplo

En el siguiente ejemplo se muestra el `running-config` el archivo se ha copiado correctamente en `startup-config` archivo:

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

Paso 3: Copie la imagen de NX-OS en el switch Cisco S2 y reinicie

1. Copie la imagen NX-OS en el switch S2.

Muestra el 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 de modo que la nueva versión se cargue la próxima vez que se reinicie el conmutador S2.

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

Muestra el 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 acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencias de comandos NX-OS de Cisco Nexus serie 3000"](#).

Se le solicitará que reinicie el sistema.

Muestra el 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 nuevo número de versión del NX-OS está en el switch:

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/old-licenses/library.txt>.

Software

BIOS: version 08.38

NXOS: version 9.3(4)

BIOS compile time: 05/29/2020

NXOS image file is: bootflash:///nxos.9.3.4.bin

NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]

Hardware

cisco 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 los switches y puertos

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

```
system switch ethernet show
```

Muestra el 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. Compruebe que los puertos del switch funcionan en buen estado y operativo después del reinicio:

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

Muestra el ejemplo

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

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

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						

3. Vuelva a comprobar que no haya problemas de switch de almacenamiento o cableado con el clúster:

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

Muestra el 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 el conmutador S1 RCF on.
5. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

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

Cisco Nexus 3132Q-V

Descripción general

Descripción general de la instalación y la configuración de los switches Cisco Nexus 3132Q-V.

Los switches Cisco Nexus 3132Q-V se pueden utilizar como switches de clúster en su clúster AFF o FAS. Los switches de clúster permiten crear clústeres de ONTAP con más de dos nodos.

Información general de configuración inicial

Para configurar inicialmente un switch Cisco Nexus 3132Q-V en sistemas que ejecutan ONTAP, siga estos pasos:

1. ["Hoja de trabajo completa del cableado Cisco Nexus 3132Q-V."](#) La hoja de cálculo de cableado de ejemplo proporciona ejemplos de asignaciones de puertos recomendadas desde los switches a las controladoras. La hoja de datos en blanco proporciona una plantilla que puede utilizar para configurar su clúster.
2. ["Instale un switch de clúster Cisco Nexus 3132Q-V en un armario de NetApp"](#). Instale el switch Cisco Nexus 3132Q-V y el panel de paso a través en un armario de NetApp con los soportes estándar que se incluyen con el switch.
3. ["Configure el switch Cisco Nexus 3132Q-V."](#) Instalar y configurar el switch Cisco Nexus 3132Q-V.
4. ["Prepare la instalación del software NX-OS y del archivo de configuración de referencia"](#). Prepare la instalación del software NX-OS y del archivo de configuración de referencia (RCF).
5. ["Instale el software NX-OS"](#). Siga este procedimiento para instalar el software NX-OS en el switch de clúster Nexus 3132Q-V.
6. ["Instalación del archivo de configuración de referencia \(RCF\)"](#). Siga este procedimiento para instalar el RCF después de configurar por primera vez el interruptor Nexus 3132Q-V. También puede utilizar este procedimiento para actualizar la versión de RCF.

Información adicional

Antes de iniciar la instalación o el mantenimiento, asegúrese de revisar lo siguiente:

- ["Requisitos de configuración"](#)
- ["Documentación requerida"](#)
- ["Requisitos de Smart Call Home"](#)

Requisitos de configuración para switches Cisco Nexus 3132Q-V.

Para la instalación y el mantenimiento del switch Cisco Nexus 3132Q-V, asegúrese de revisar los requisitos de red y configuración.

Requisitos de configuración

Para configurar el clúster, necesita el número y el tipo de cables y conectores de cable adecuados para los switches. Según el tipo de switch que esté configurando inicialmente, debe conectarse al puerto de la consola del switch con el cable de consola incluido; también debe proporcionar información de red específica.

Requisitos de red

Necesita la siguiente información de red para todas las configuraciones de los switches:

- Subred IP para el tráfico de red de gestión.
- Nombres de host y direcciones IP para cada una de las controladoras del sistema de almacenamiento y todos los switches aplicables.
- La mayoría de las controladoras del sistema de almacenamiento se gestionan a través de la interfaz e0M mediante la conexión al puerto de servicio Ethernet (icono de llave inglesa). En los sistemas A800 y A700 de AFF de AFF, la interfaz e0M utiliza un puerto Ethernet dedicado.

Consulte la ["Hardware Universe"](#) para obtener la información más reciente.

Requisitos de documentación para los switches Cisco Nexus 3132Q-V.

Para la instalación y el mantenimiento del switch Cisco Nexus 3132Q-V, asegúrese de revisar toda la documentación recomendada.

Documentación de los switches

Para configurar los switches Cisco Nexus 3132Q-V, necesita la siguiente documentación de la ["Compatibilidad con los 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 acerca de los requisitos del sitio, detalles del switch de hardware y las opciones de instalación.
<i>Guías de configuración del software del switch Cisco Nexus serie 3000</i> (elija la guía para la versión NX-OS instalada en los switches)	Proporciona la información inicial de configuración del switch que necesita para poder configurar el switch para el funcionamiento de ONTAP.
<i>Guía de actualización y degradación de software NX-OS de Cisco Nexus 3000 Series</i> (elija la guía para la versión de NX-OS instalada en los switches)	Proporciona información sobre cómo degradar el switch a software de switch compatible con ONTAP, si es necesario.
<i>Cisco Nexus 3000 Series NX-OS Command Reference Master Index</i>	Proporciona vínculos a las diferentes referencias de comandos proporcionadas por Cisco.
<i>Cisco Nexus 3000 MIBs Reference</i>	Describe los archivos de la base de datos de información de gestión (MIB) para los switches Nexus 3000.
<i>Referencia de mensajes del sistema NX-OS serie Nexus 3000</i>	Describe los mensajes del sistema de los switches Cisco Nexus serie 3000, los 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 Cisco Nexus serie 3000 NX-OS (elija las notas para la versión de NX-OS instalada en los switches)</i>	Describe las funciones, errores y limitaciones de Cisco Nexus 3000 Series.
Información sobre cumplimiento de normativas y seguridad de Cisco Nexus 6000, Cisco Nexus 5000 Series, Cisco Nexus 3000 Series y Cisco Nexus 2000 Series	Proporciona información legal, de seguridad y cumplimiento de normativas de agencias 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 desde la ["Centro de documentación de ONTAP 9"](#).

Nombre	Descripción
Específicos del controlador <i>instrucciones de instalación y configuración</i>	Describe cómo instalar el hardware de NetApp.
Documentación de ONTAP	Proporciona información detallada sobre todos los aspectos de las versiones de ONTAP.
"Hardware Universe"	Ofrece información de compatibilidad y configuración de hardware de NetApp.

Kit de raíl y documentación del armario

Para instalar un switch Cisco de 3132Q-V en un armario de NetApp, consulte la siguiente documentación de hardware.

Nombre	Descripción
"Armario del sistema 42U, guía detallada"	Describe las FRU asociadas al armario del sistema 42U, y proporciona instrucciones de mantenimiento y sustitución de FRU.
"Instale el switch Cisco Nexus 3132Q-V en un armario de NetApp"	Describe cómo instalar un switch Cisco Nexus 3132Q-V en un armario de cuatro parantes de NetApp.

Requisitos de Smart Call Home

Para utilizar la función de inicio de llamada inteligente, revise las siguientes directrices.

Smart Call Home supervisa los componentes de hardware y software de su red. Cuando se produce una configuración de sistema crítica, genera una notificación basada en correo electrónico y genera una alerta a

todos los destinatarios que están configurados en el perfil de destino. 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 el conmutador de red de clúster para aprovechar la función integrada de soporte Smart Call Home de Cisco.

Antes de poder utilizar Smart Call Home, tenga en cuenta las siguientes consideraciones:

- Debe haber un servidor de correo electrónico.
- El switch debe tener conectividad IP con el servidor de correo electrónico.
- Se debe configurar el nombre del contacto (contacto del servidor SNMP), el número de teléfono y la dirección de la calle. Esto es necesario para determinar el origen de los mensajes recibidos.
- Un ID de CCO debe estar asociado con un contrato de servicio Cisco SMARTnet adecuado para su empresa.
- El servicio Cisco SMARTnet debe estar en su lugar para que el dispositivo se registre.

La ["Sitio de soporte de Cisco"](#) Contiene información acerca de los comandos para configurar Smart Call Home.

Instale el hardware

Hoja de trabajo completa del cableado Cisco Nexus 3132Q-V.

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

La hoja de cálculo de cableado de ejemplo proporciona ejemplos de asignaciones de puertos recomendadas desde los switches a las controladoras. La hoja de datos en blanco proporciona una plantilla que puede utilizar para configurar su clúster.

Cada switch puede configurarse como un único puerto de 40 GbE o como 4 puertos de 10 GbE.

Hoja de trabajo para el cableado de muestra

La definición de puerto de ejemplo de cada par de conmutadores es la siguiente:

Switch de clúster a		Switch del clúster B	
Puerto del switch	Uso de nodos y puertos	Puerto del switch	Uso de nodos y puertos
1	4 nodos 10G/40G	1	4 nodos 10G/40G
2	4 nodos 10G/40G	2	4 nodos 10G/40G
3	4 nodos 10G/40G	3	4 nodos 10G/40G
4	4 nodos 10G/40G	4	4 nodos 10G/40G
5	4 nodos 10G/40G	5	4 nodos 10G/40G
6	4 nodos 10G/40G	6	4 nodos 10G/40G

Switch de clúster a		Switch del clúster B	
7	4 nodos 10G/40G	7	4 nodos 10G/40G
8	4 nodos 10G/40G	8	4 nodos 10G/40G
9	4 nodos 10G/40G	9	4 nodos 10G/40G
10	4 nodos 10G/40G	10	4 nodos 10G/40G
11	4 nodos 10G/40G	11	4 nodos 10G/40G
12	4 nodos 10G/40G	12	4 nodos 10G/40G
13	4 nodos 10G/40G	13	4 nodos 10G/40G
14	4 nodos 10G/40G	14	4 nodos 10G/40G
15	4 nodos 10G/40G	15	4 nodos 10G/40G
16	4 nodos 10G/40G	16	4 nodos 10G/40G
17	4 nodos 10G/40G	17	4 nodos 10G/40G
18	4 nodos 10G/40G	18	4 nodos 10G/40G
19	40 G nodo 19	19	40 G nodo 19
20	40 G nodo 20	20	40 G nodo 20
21	40 G nodo 21	21	40 G nodo 21
22	40 G nodo 22	22	40 G nodo 22
23	40 G nodo 23	23	40 G nodo 23
24	40 G nodo 24	24	40 G nodo 24
25 hasta 30	Reservado	25 hasta 30	Reservado
31	40 G de ISL al puerto 31 del switch B.	31	40 G de ISL para cambiar al puerto 31
32	40 G de ISL al puerto 32 del switch B.	32	40 G de ISL para cambiar al puerto 32

Hoja de trabajo de cableado en blanco

Puede utilizar la hoja de datos de cableado vacía para documentar las plataformas que se admiten como nodos de un clúster. La sección *Cluster Connections* del "Hardware Universe" define los puertos de clúster que utiliza la plataforma.

Switch de clúster a		Switch del clúster B	
Puerto del switch	Uso del nodo/puerto	Puerto del switch	Uso del nodo/puerto
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	

Switch de clúster a		Switch del clúster B	
20		20	
21		21	
22		22	
23		23	
24		24	
25 hasta 30	Reservado	25 hasta 30	Reservado
31	40 G de ISL al puerto 31 del switch B.	31	40 G de ISL para cambiar al puerto 31
32	40 G de ISL al puerto 32 del switch B.	32	40 G de ISL para cambiar al puerto 32

Configure el switch Cisco Nexus 3132Q-V.

Siga este procedimiento para configurar el switch Cisco Nexus 3132Q-V.

Lo que necesitará

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones correspondientes del NX-OS y del archivo de configuración de referencia (RCF).
- La versión aplicable de NX-OS, descargada del ["Descarga de software de Cisco"](#) página.
- Se requiere documentación del switch de red, documentación de la controladora y documentación de ONTAP. Para obtener más información, consulte ["Documentación requerida"](#).
- Las licencias aplicables, la información de configuración y red, y los cables.
- Hojas de datos de cableado completadas. Consulte ["Hoja de trabajo completa del cableado Cisco Nexus 3132Q-V."](#)
- Archivos RCF de red de gestión y red de clúster de NetApp aplicables, descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#) para los switches que reciba. Todos los switches de red de gestión y red de clúster de Cisco llegan con la configuración predeterminada de fábrica de Cisco. Estos conmutadores también tienen la versión actual del software NX-OS, pero no tienen cargados los RCF.

Pasos

1. Monte en rack la red del clúster y los switches de red de gestión y las controladoras.


Si está instalando el...	Realice lo siguiente...
Cisco Nexus 3132Q-V en un armario del sistema de NetApp	Consulte la guía <i>instalación de un switch de clúster Cisco Nexus 3132Q-V y panel de paso a través en un armario de NetApp</i> para obtener instrucciones sobre cómo instalar el switch en un armario de NetApp.


Si está instalando el...	Realice lo siguiente...
Equipo en un bastidor de Telco	Consulte los procedimientos proporcionados en las guías de instalación del hardware del switch y las instrucciones de instalación y configuración de NetApp.

- Conecte los cables de la red de clústeres y los switches de red de gestión a las controladoras mediante la hoja de datos de cableado completada, como se describe en ["Hoja de trabajo completa del cableado Cisco Nexus 3132Q-V."](#)
- Encienda la red de clúster y los switches de red de gestión y las controladoras.
- Realice una configuración inicial de los switches de red de clúster.

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

Prompt	Respuesta
¿Desea anular el aprovisionamiento automático y continuar con la configuración normal? (sí/no)	Responda con sí . El valor predeterminado es no
¿Desea aplicar un estándar de contraseña segura? (sí/no)	Responda con sí . El valor predeterminado es yes.
Introduzca la contraseña para el administrador:	La contraseña predeterminada es "admin"; debe crear una nueva contraseña segura. Se puede rechazar una contraseña débil.
¿Desea introducir el cuadro de diálogo de configuración básica? (sí/no)	Responda con sí en la configuración inicial del interruptor.
¿Crear otra cuenta de inicio de sesión? (sí/no)	Su respuesta depende de las políticas de su sitio con respecto a los administradores alternativos. El valor predeterminado es no .
¿Configurar cadena de comunidad SNMP de solo lectura? (sí/no)	Responda con no . El valor predeterminado es no
¿Configurar cadena de comunidad SNMP de lectura y escritura? (sí/no)	Responda con no . El valor predeterminado es no
Introduzca el nombre del switch.	El nombre del conmutador está limitado a 63 caracteres alfanuméricos.

Prompt	Respuesta
¿Continuar con la configuración de administración fuera de banda (mgmt0)? (sí/no)	Responda con sí (el valor predeterminado) en ese indicador. En el símbolo de sistema mgmt0 IPv4 address:, introduzca su dirección IP: ip_address.
¿Configurar la puerta de enlace predeterminada? (sí/no)	Responda con sí . En la dirección IPv4 de la solicitud default-Gateway:, introduzca su default_Gateway.
¿Configurar las opciones avanzadas de IP? (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. El valor predeterminado es yes.</p> <div>  <p>Se recomienda SSH cuando se utilice el Monitor de estado del conmutador de clúster (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.</p> </div>
Introduzca el tipo de clave SSH que desea generar (dsa/rsa/rsa1).	El valor predeterminado es rsa .
Introduzca el número de bits de clave (1024-2048).	Introduzca los bits clave de 1024-2048.
¿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 (cerrada/nohut):	Responda con nohut . El valor predeterminado es nohut.
Configurar el perfil del sistema COPP (estricto/moderado/indulgente/denso):	Responda con estricto . El valor predeterminado es estricto.
¿Desea editar la configuración? (sí/no)	Debería ver la nueva configuración en este momento. Revise y realice los cambios necesarios en la configuración que acaba de introducir. Si está satisfecho con la configuración, responda no en el indicador. Responda con sí si desea editar los ajustes de configuración.

Prompt	Respuesta
¿Utilizar esta configuración y guardarla? (sí/no)	<p>Responda con sí para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.</p> <div>  <p>Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador.</p> </div>

- Compruebe las opciones de configuración que ha realizado en la pantalla que aparece al final de la instalación y asegúrese de guardar la configuración.
- Compruebe la versión de los switches de red del clúster y, si es necesario, descargue la versión del software compatible con NetApp en los switches de la ["Descarga de software de Cisco"](#) página.

El futuro

["Prepare la instalación de NX-OS y RCF"](#).

Instale un switch de clúster Cisco Nexus 3132Q-V en un armario de NetApp

En función de la configuración, es posible que necesite instalar el switch y el panel de paso a través de Cisco Nexus 3132Q-V en un armario de NetApp con los soportes estándar que se incluyen con el switch.

Lo que necesitará

- Los requisitos iniciales de preparación, el contenido del kit y las precauciones de seguridad del ["Guía de instalación de hardware de Cisco Nexus serie 3000"](#). Revise estos documentos antes de comenzar el procedimiento.
- El kit de panel de paso a través, disponible en NetApp (número de pieza X8784-R6). El kit del panel de paso a través de NetApp contiene el siguiente hardware:
 - Un panel de supresión de paso a través
 - Cuatro tornillos de 10-32 x 0,75
 - Cuatro tuercas de 10-32 abrazaderas
- Ocho tornillos 10-32 ó 12-24 y tuercas de sujeción para montar los soportes y rieles deslizantes en los postes del armario delantero y trasero.
- Kit de guías estándar de Cisco para instalar el switch en un armario de NetApp.



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

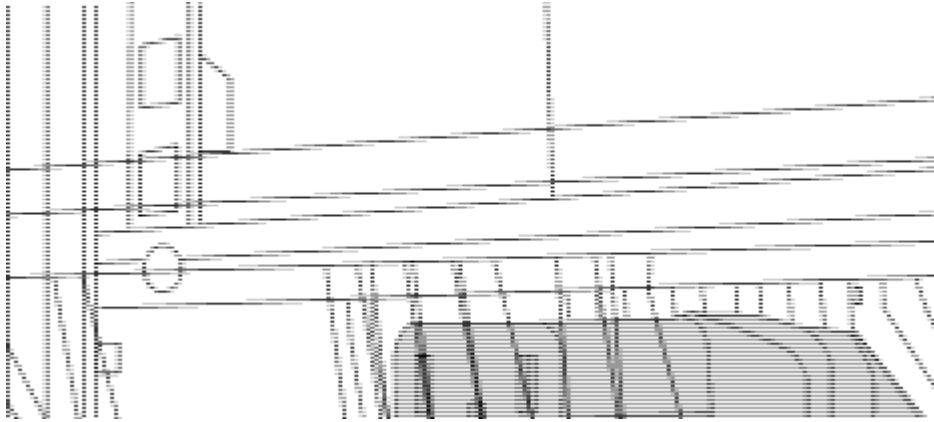
Pasos

- Instale el panel de borrado de paso en el armario de NetApp.
 - Determine la ubicación vertical de los interruptores y el panel de supresión en el armario.

En este procedimiento, el panel de limpieza se instalará en U40.
 - Instale dos tuercas de abrazadera a cada lado en los orificios cuadrados adecuados para los rieles

delanteros del armario.

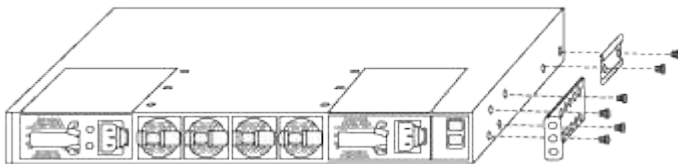
- c. Centre el panel verticalmente para evitar intrusiones en el espacio adyacente del bastidor y, a continuación, apriete los tornillos.
- d. Inserte los conectores hembra de ambos cables puente de 48 pulgadas desde la parte posterior del panel y a través del conjunto del cepillo.



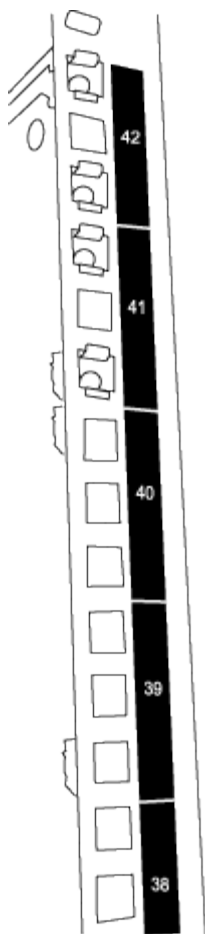
(1) conector hembra del cable puente.

2. Instale los soportes de montaje en rack en el chasis del switch Nexus 3132Q-V.

- a. Coloque un soporte de montaje de rack frontal en un lado del chasis del switch de modo que el oído de montaje esté alineado con la placa frontal del chasis (en el lado de la fuente de alimentación o del ventilador) y, a continuación, utilice cuatro tornillos M4 para conectar el soporte al chasis.



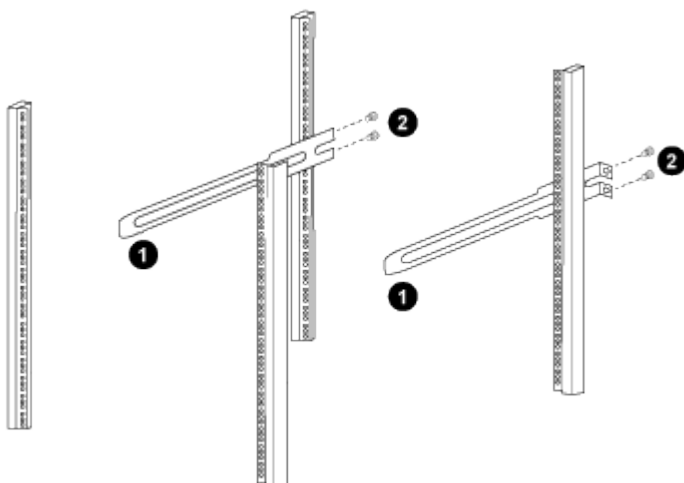
- b. Repita el paso 2a con el otro soporte de montaje en bastidor delantero en el otro lado del interruptor.
 - c. Instale el soporte de montaje en bastidor trasero en el chasis del interruptor.
 - d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del interruptor.
3. Instale las tuercas de abrazadera en las ubicaciones de los orificios cuadrados de los cuatro postes de IEA.



Los dos interruptores 3132Q-V siempre se montarán en la parte superior 2U del armario RU41 y 42.

4. Instale los rieles deslizantes en el armario.

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



(1) mientras desliza suavemente el raíl deslizante, alinéelo con los orificios de los tornillos del rack.

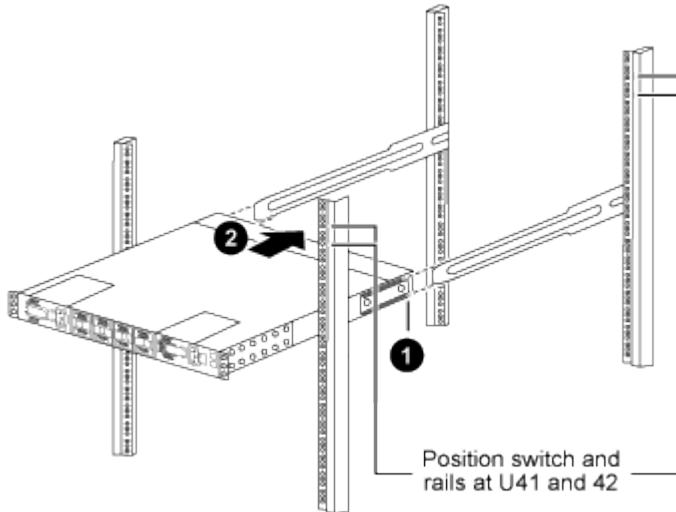
(2) apriete los tornillos de las guías deslizantes a los postes del armario.

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



Este paso requiere dos personas: Una persona para sostener el interruptor desde la parte frontal y otra para guiar el interruptor hacia los rieles deslizantes traseros.

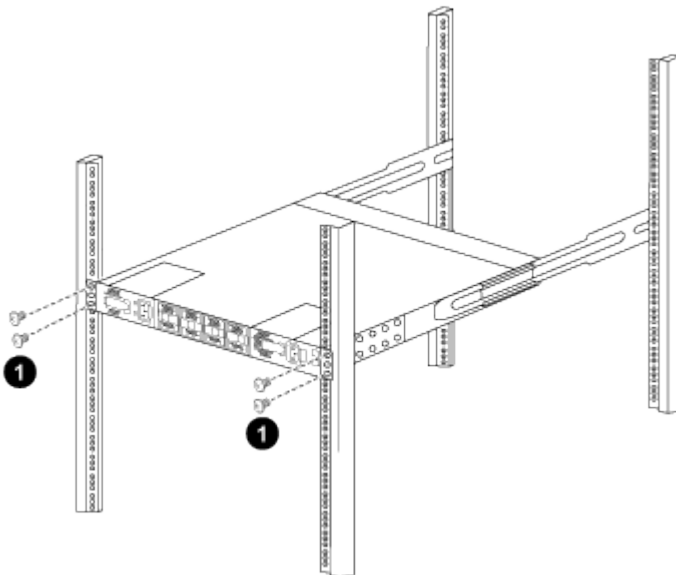
- a. Coloque la parte posterior del interruptor en RU41.



(1) a medida que el chasis se empuja hacia los postes traseros, alinee las dos guías de montaje en bastidor trasero con los rieles deslizantes.

(2) deslice suavemente el interruptor hasta que los soportes de montaje del bastidor delantero estén a ras con los postes delanteros.

- b. Conecte el interruptor al armario.



(1) con una persona sujetando la parte delantera del chasis, la otra persona debe apretar completamente los cuatro tornillos traseros a los postes del armario.

- a. Con el chasis apoyado ahora 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 mantener la parte frontal del segundo interruptor durante el proceso de instalación.

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



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

8. Conecte el puerto de administración de cada switch 3132Q-V a cualquiera de los switches de administración (si se solicita) o conéctelos directamente a la red de administración.

El puerto de gestión es el puerto superior derecho ubicado en el lado PSU del switch. El cable CAT6 para cada switch debe enrutarse a través del panel de paso a través después de instalar los switches para conectarse a los switches de administración o a la red de gestión.

Revise las consideraciones sobre el cableado y la configuración

Antes de configurar su switch Cisco 3132Q-V, revise las siguientes consideraciones.

Compatibilidad con los puertos NVIDIA CX6, CX6-DX y Ethernet de CX7 Gb

Si se conecta un puerto de switch a un controlador ONTAP mediante los puertos NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) o ConnectX-7 (CX7), debe codificar de forma fija la velocidad del puerto del switch.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Consulte "[Hardware Universe](#)" para obtener más información sobre los puertos de switch.

Configurar el software

Prepare la instalación del software NX-OS y del archivo de configuración de referencia

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 de 10 GbE e0a y.. e0b.

Consulte "[Hardware Universe](#)" para verificar los puertos de clúster correctos en sus plataformas.



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

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

- Los nombres de los dos switches Cisco son `cs1` y.. `cs2`.
- Los nombres de nodo son `cluster1-01` y.. `cluster1-02`.
- Los nombres de 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`.
- La `cluster1::*>` prompt indica el nombre del clúster.

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Pasos

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

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

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



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

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

```
set -privilege advanced
```

El aviso avanzado (***>**) aparece.

3. Muestre cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster:

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

Muestra el ejemplo

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
-----	-----	-----	-----	
cluster1-02/cdp				
C3132Q-V	e0a	cs1	Eth1/2	N3K-
C3132Q-V	e0b	cs2	Eth1/2	N3K-
cluster1-01/cdp				
C3132Q-V	e0a	cs1	Eth1/1	N3K-
C3132Q-V	e0b	cs2	Eth1/1	N3K-
C3132Q-V				

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

a. Mostrar los atributos del puerto de red:

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

Muestra el ejemplo

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

```
Node: 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						

b. Mostrar información acerca de las LIF:

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

Muestra el ejemplo

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

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

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

5. Haga ping en las LIF de clúster remoto:

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

Muestra el ejemplo

```
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)
```

6. Compruebe que el auto-revert El comando está habilitado en todos los LIF de clúster:

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

Muestra el ejemplo

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

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

El futuro

["Instale el software NX-OS"](#).

Instale el software NX-OS

Siga este procedimiento para instalar el software NX-OS en el switch de clúster Nexus 3132Q-V.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).

Documentación sugerida

- ["Switch Ethernet de Cisco"](#). Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.
- ["Switches Cisco Nexus serie 3000"](#). Consulte las guías de actualización y software adecuadas disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de switches de Cisco.

Instale el software

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Asegúrese de completar el procedimiento en ["Prepare la instalación del software NX-OS y del archivo de configuración de referencia"](#)y, a continuación, siga los pasos que se indican a continuación.

Pasos

1. Conecte el switch de clúster a la red de gestión.

2. Utilice la `ping` Comando para verificar la conectividad con el servidor que aloja el software NX-OS y el RCF.

Muestra el ejemplo

```
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. Copie el software NX-OS en el switch Nexus 3132Q-V utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información acerca de los comandos de Cisco, consulte la guía adecuada en ["Guías de referencia de comandos Cisco Nexus serie 3000 NX-OS"](#).

Muestra el 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: xxxxxxxx
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.
```

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

```
show version
```

Muestra el ejemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, 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 04.25
  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 Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash: 15137792 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
Reason: Reset Requested by CLI command reload
System version: 9.3(3)
Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
cs2#
```

5. Instale la imagen NX-OS.

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

Muestra el ejemplo

```
cs2# install all nxos bootflash:nxos.9.3.4.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      v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(01/28/2020)  no

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

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[ ] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[ ] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[ ] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[ ] 100% -- SUCCESS
```

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

```
cs2#
```

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

```
show version
```

```
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 04.25
  NXOS: version 9.3(4)
  BIOS compile time: 05/22/2019
  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 Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash: 15137792 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
Reason: Reset Requested by CLI command reload
System version: 9.3(4)
Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s) :

cs2#
```

El futuro

["Instalación del archivo de configuración de referencia \(RCF\)".](#)

Instalación del archivo de configuración de referencia (RCF)

Siga este procedimiento para instalar el RCF después de configurar por primera vez el interruptor Nexus 3132Q-V. También puede utilizar este procedimiento para actualizar la versión de RCF.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El archivo de configuración de referencia actual (RCF).
- Una conexión de consola al conmutador, necesaria para instalar el RCF.
- ["Switch Ethernet de Cisco"](#). Consulte la tabla de compatibilidad del conmutador para conocer las versiones ONTAP y RCF admitidas. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis del comando en el RCF y la que se encuentra en las versiones de NX-OS.
- ["Switches Cisco Nexus serie 3000"](#). Consulte las guías de actualización y software adecuadas disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de switches de Cisco.

Instale el archivo

Acerca de los ejemplos

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

- Los nombres de los dos switches Cisco son `cs1` y `cs2`.
- Los nombres de nodo son `cluster1-01`, `cluster1-02`, `cluster1-03`, y `cluster1-04`.
- Los nombres de 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`.

- La `cluster1::*>` prompt indica el nombre del clúster.

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Durante este procedimiento no se necesita ningún enlace entre switches (ISL) operativo. Esto se debe a que los cambios en la versión de RCF pueden afectar temporalmente a la conectividad ISL. Para garantizar operaciones de clúster no disruptivas, el siguiente procedimiento migra todas las LIF del clúster al switch de partner operativo mientras realiza los pasos del switch de destino.

Asegúrese de completar el procedimiento en "[Prepare la instalación del software NX-OS y del archivo de configuración de referencia](#)", y, a continuación, siga los pasos que se indican a continuación.

Paso 1: Compruebe el estado del puerto

1. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```


Muestra el ejemplo

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				
-----	-----	-----	-----	-----
cluster1-01/cdp				
	e0a	cs1	Ethernet1/7	N3K-
C3132Q-V				
	e0d	cs2	Ethernet1/7	N3K-
C3132Q-V				
cluster1-02/cdp				
	e0a	cs1	Ethernet1/8	N3K-
C3132Q-V				
	e0d	cs2	Ethernet1/8	N3K-
C3132Q-V				
cluster1-03/cdp				
	e0a	cs1	Ethernet1/1/1	N3K-
C3132Q-V				
	e0b	cs2	Ethernet1/1/1	N3K-
C3132Q-V				
cluster1-04/cdp				
	e0a	cs1	Ethernet1/1/2	N3K-
C3132Q-V				
	e0b	cs2	Ethernet1/1/2	N3K-
C3132Q-V				
cluster1::*>				

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

a. Compruebe que todos los puertos del clúster tengan el estado correcto:

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

Muestra el ejemplo

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

```
Node: 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

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

cluster1::*>

b. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

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

Muestra el ejemplo

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

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

Cluster				
	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			

```
cluster1::*>
```

c. Compruebe que el clúster muestra información de ambos switches de clúster:

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

Muestra el ejemplo

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
cs1                                     cluster-network     10.0.0.1
NX3132QV
    Serial Number: FOXXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                        9.3(4)
    Version Source: CDP

cs2                                     cluster-network     10.0.0.2
NX3132QV
    Serial Number: FOXXXXXXXXGD
    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.
```



Para ONTAP 9.8 y versiones posteriores, utilice el comando `system switch ethernet show -is-monitoring-enabled-operational true`.

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

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

Asegúrese de que la reversión automática esté deshabilitada después de ejecutar este comando.

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

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

5. Comprobar que los puertos del clúster han migrado a los puertos alojados en el switch cs1 del clúster. Esto puede tardar unos segundos.

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

Muestra el ejemplo

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0a false			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0a false			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0a false			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0a false			

```
cluster1::*>
```

6. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el 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
cluster1::*>
```

Paso 2: Configurar y verificar la configuración

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

```
show running-config
```

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



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

- a. Limpie la configuración:

Muestra el ejemplo

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Reinicie el conmutador:

Muestra el ejemplo

```
(cs2)# reload

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

3. Copie el RCF en el bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

Muestra el ejemplo

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3132QV_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)...
```

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

Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

Muestra el ejemplo

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

5. Examine el resultado del banner desde el `show banner motd` comando. Debe leer y seguir las instrucciones que se indican en **Notas importantes** para garantizar la configuración y el funcionamiento correctos del interruptor.

Muestra el ejemplo

```
cs2# show banner motd
```

```
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Cisco Nexus 3132Q-V
* Filename  : Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
* Date      : Nov-02-2020
* Version   : v1.6
*
* Port Usage : Breakout configuration
* Ports 1- 6: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4,int e1/4/1-4, e1/5/1-4, e1/6/1-4
* Ports 7-30: 40GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
*
* IMPORTANT NOTES
* - Load Nexus_3132QV_RCF_v1.6-Cluster-HA.txt for non breakout
config
*
* - This RCF utilizes QoS and requires specific TCAM configuration,
requiring
*   cluster switch to be rebooted before the cluster becomes
operational.
*
* - Perform the following steps to ensure proper RCF installation:
*
*   (1) Apply RCF, 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...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*
*   (4) Save running-configuration again
*
```

```

* - If running NX-OS versions 9.3(5) 9.3(6), 9.3(7), or 9.3(8)
*   - Downgrade the NX-OS firmware to version 9.3(5) or earlier if
*     NX-OS using a version later than 9.3(5).
*   - Do not upgrade NX-OS prior to applying v1.9 RCF file.
*   - After the RCF is applied and switch rebooted, then proceed to
upgrade
*     NX-OS to version 9.3(5) or later.
*
* - If running 9.3(9) 10.2(2) or later the RCF can be applied to the
switch
*   after the upgrade.
*
* - Port 1 multiplexed H/W configuration options:
*   hardware profile front portmode qsfp      (40G H/W port 1/1 is
active - default)
*   hardware profile front portmode sfp-plus  (10G H/W ports 1/1/1
- 1/1/4 are active)
*   hardware profile front portmode qsfp      (To reset to QSFP)
*
*****
*****

```

6. Compruebe que el archivo RCF es la versión más reciente correcta:

```
show running-config
```

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

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

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



Para conocer los pasos sobre cómo conectar sus puertos 10GbE después de una actualización de RCF, consulte el artículo de la base de conocimientos ["Los puertos 10GbE de un switch de clúster Cisco 3132Q no se conectan"](#).

7. Después de comprobar que las versiones de RCF y los ajustes del switch son correctos, copie el archivo running-config en el archivo startup-config.

Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) guías.

Muestra el ejemplo

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

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

Muestra el ejemplo

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

9. Aplique el mismo RCF y guarde la configuración en ejecución por segunda vez.

Muestra el ejemplo

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
cs2# copy running-config startup-config
[#####] 100% Copy complete
```

10. Compruebe el estado de los puertos del clúster en el clúster.
- a. Compruebe que los puertos del clúster estén en buen estado en todos los nodos del clúster:

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

Muestra el 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					
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					

b. Compruebe el estado del switch del clúster.

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

Muestra el ejemplo

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

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

cluster1-01/cdp			
	e0a	cs1	Ethernet1/7
N3K-C3132Q-V			
	e0d	cs2	Ethernet1/7
N3K-C3132Q-V			
cluster01-2/cdp			
	e0a	cs1	Ethernet1/8
N3K-C3132Q-V			
	e0d	cs2	Ethernet1/8
N3K-C3132Q-V			
cluster01-3/cdp			
	e0a	cs1	Ethernet1/1/1
N3K-C3132Q-V			
	e0b	cs2	Ethernet1/1/1
N3K-C3132Q-V			
cluster1-04/cdp			
	e0a	cs1	Ethernet1/1/2
N3K-C3132Q-V			
	e0b	cs2	Ethernet1/1/2
N3K-C3132Q-V			

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

Switch	Type	Address
Model		

cs1	cluster-network	10.233.205.90

N3K-C3132Q-V		
Serial Number: FOXXXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
9.3(4)		
Version Source: CDP		
cs2	cluster-network	10.233.205.91

```

N3K-C3132Q-V
  Serial Number: FOXXXXXXXXGS
    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.

```



Para ONTAP 9.8 y versiones posteriores, utilice el comando `system switch ethernet show -is-monitoring-enabled-operational true`.

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



```

2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.

```

+



Los nodos del clúster pueden tardar hasta 5 minutos en informar en buen estado.

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

Muestra el ejemplo

```

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

```

12. Comprobar que las LIF del clúster han migrado a los puertos alojados en el switch cs2. Esto puede tardar unos segundos.

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

Muestra el ejemplo

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0d	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	false		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
cluster1::*>
```

13. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el 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 del 1 al 10 en el interruptor cs1.
15. Habilite la reversión automática en las LIF del clúster.

Muestra el ejemplo

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

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

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

Paso 3: Verificar la configuración

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

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

Muestra el 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. Compruebe que el ISL entre cs1 y cs2 funciona:

```
show port-channel summary
```

Muestra el ejemplo

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
      Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
cs1#
```

3. Compruebe que las LIF del clúster han vuelto a su puerto de inicio:

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

Muestra el ejemplo

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

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

Cluster				
	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		

```
cluster1::*>
```

4. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el 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

```
cluster1::*>
```

5. Haga ping en las interfaces de clúster remoto para verificar la conectividad:

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

6. Para ONTAP 9.8 y versiones posteriores, habilite la función de recogida de registros de control de estado

del switch de Ethernet para recopilar archivos de registro relacionados con el switch mediante los comandos:

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

```
system switch ethernet log enable-collection
```

a. Introduzca: `system switch ethernet log setup-password`

Muestra el ejemplo

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

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

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

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

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

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

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

b. Introduzca: `system switch ethernet log enable-collection`

Muestra el ejemplo

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

```
Do you want to enable cluster log collection for all nodes in the  
cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

7. Para las versiones 9.5P16, 9.6P12 y 9.7P10 de ONTAP y versiones posteriores de parches, habilite la función de recopilación de registros del monitor de estado del switch Ethernet para recopilar archivos de registro relacionados con el switch mediante los comandos:

```
system cluster-switch log setup-password y..
```

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

- a. Introduzca: `system cluster-switch log setup-password`

Muestra el ejemplo

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

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

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

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

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

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

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

b. Introduzca: `system cluster-switch log enable-collection`

Muestra el ejemplo

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

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

Enabling cluster switch log collection.

cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

Recopilación de registro de supervisión del estado del switch Ethernet

Es posible usar la función de recopilación de registros para recoger archivos de registro relacionados con switches en ONTAP.

El monitor de estado del switch Ethernet (CSHM) es responsable de garantizar el estado operativo de los conmutadores de red del clúster y de almacenamiento y de recopilar registros del switch para fines de depuración. Este procedimiento lo guía a través del proceso de configuración e inicio de la recopilación de registros detallados de **Soporte** desde el switch e inicia una recopilación por hora de datos **Periódicos** que es recopilada por AutoSupport.

Antes de empezar

- Compruebe que ha configurado su entorno mediante el conmutador de clúster de Cisco 3132Q-V **CLI**.
- La monitorización del estado del interruptor debe estar activada para el interruptor. Verifique esto asegurándose de que el `Is Monitored:` el campo se establece en **true** en la salida del `system switch ethernet show` comando.

Pasos

1. Cree una contraseña para la función de recogida de registros de monitor de estado del switch Ethernet:

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


Muestra el ejemplo

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

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

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

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

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

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

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

2. Para iniciar la recopilación de registros, ejecute el siguiente comando, sustituyendo EL DISPOSITIVO por el conmutador utilizado en el comando anterior. Esto inicia ambos tipos de recopilación de registros: Los registros detallados de **Support** y una recopilación horaria de datos **Periódicos**.

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

Muestra el ejemplo

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Espere 10 minutos y compruebe que se complete la recogida de registros:

```
system switch ethernet log show
```



Si alguno de estos comandos devuelve un error o si la recogida de registros no se completa, póngase en contacto con el soporte de NetApp.

Resolución de problemas

Si se encuentra con alguno de los siguientes estados de error informados por la función de recopilación de registros (visible en la salida de `system switch ethernet log show`), pruebe los pasos de depuración correspondientes:

Estado de error de recopilación de registros	Resolución
Las claves RSA no están presentes	Vuelva a generar las claves SSH de ONTAP. Póngase en contacto con el soporte de NetApp.
error de contraseña de cambio	Verifique las credenciales, pruebe la conectividad SSH y vuelva a generar las claves SSH de ONTAP. Revise la documentación del switch o póngase en contacto con el soporte de NetApp para obtener instrucciones.
Las claves ECDSA no están presentes para FIPS	Si el modo FIPS está activado, es necesario generar claves ECDSA en el conmutador antes de volver a intentarlo.

registro preexistente encontrado	Elimine el archivo de recopilación de registros anterior del conmutador.
error de registro de volcado del interruptor	Asegúrese de que el usuario del conmutador tiene permisos de recopilación de registros. Consulte los requisitos previos anteriores.

Configurar SNMPv3

Siga este procedimiento para configurar SNMPv3, que admite la monitorización del estado del switch Ethernet (CSHM).

Acerca de esta tarea

Los siguientes comandos configuran un nombre de usuario SNMPv3 en switches Cisco 3132Q-V.

- Para **sin autenticación**: `snmp-server user SNMPv3_USER NoAuth`
- Para **autenticación MD5/SHA**: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- Para autenticación **MD5/SHA con cifrado AES/DES**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication-method usm -remote-switch-ipaddress ADDRESS`

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

Pasos

1. Configure el usuario SNMPv3 en el conmutador para que utilice autenticación y cifrado:

```
show snmp user
```

Muestra el ejemplo

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1) (Config)# show snmp user

-----
-----
                                SNMP USERS
-----
-----

User              Auth              Priv(enforce)    Groups
acl_filter
-----
-----
admin             md5              des(no)          network-admin
SNMPv3User        md5              aes-128(no)      network-operator
-----
-----

NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

User              Auth              Priv
-----
-----

(sw1) (Config)#
```

2. Configure el usuario SNMPv3 en el lado ONTAP:

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

Muestra el ejemplo

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configure CSHM para monitorizar con el nuevo usuario de SNMPv3:

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

Muestra el ejemplo

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

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N3K-C3132Q-V
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

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

4. Compruebe que el número de serie que se va a consultar con el usuario SNMPv3 recién creado es el mismo que se detalla en el paso anterior después de que se haya completado el período de sondeo de CSHM.

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

Muestra el ejemplo

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

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

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N3K-C3132Q-V
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Migrar switches

Migre un switch de clúster Cisco Nexus 5596 a un switch de clúster Cisco Nexus 3132Q-V.

Siga este procedimiento para sustituir un switch de clúster Nexus 5596 existente por un switch de clúster Nexus 3132Q-V.

Revise los requisitos

Revise los requisitos de Cisco Nexus 5596 en ["Requisitos para sustituir los switches de clúster Cisco Nexus 3132Q-V."](#)

Para obtener más información, consulte:

- ["Página de descripción de Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Sustituya el interruptor

Acerca de los ejemplos

Los ejemplos de este procedimiento describen la sustitución de los switches Nexus 5596 por switches Nexus 3132Q-V. Puede usar estos pasos (con modificaciones) para reemplazar otros switches Cisco anteriores.

El procedimiento utiliza la siguiente nomenclatura de conmutación y nodo:

- Los resultados del comando pueden variar en función de las diferentes versiones de ONTAP.
- Los interruptores Nexus 5596 que se deben sustituir son CL1 y CL2.
- Los switches Nexus 3132Q-V que sustituyen a los switches Nexus 5596 son C1 y C2.
- n1_clus1 es la primera interfaz lógica del clúster (LIF) conectada al switch del clúster 1 (CL1 o C1) para el nodo n1.
- n1_clus2 es la primera LIF del clúster conectada al switch de clúster 2 (CL2 o C2) para el nodo n1.
- n1_clus3 es la segunda LIF conectada al switch de clúster 2 (CL2 o C2) para el nodo n1.
- n1_clus4 es la segunda LIF conectada al switch de clúster 1 (CL1 o C1) para el nodo n1.
- Los nodos son n1, n2, n3 y n4.
- Los ejemplos de este procedimiento emplean cuatro nodos: Dos nodos utilizan cuatro puertos de interconexión de clúster de 10 GbE: E0a, e0b, e0c y e0d. Los otros dos nodos utilizan dos puertos de interconexión de clúster de 40/100 GbE: e4a y e4e. La ["Hardware Universe"](#) la enumera los puertos del clúster reales en las plataformas.
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) página.



Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Acerca de esta tarea

Este procedimiento cubre los siguientes escenarios:

- El clúster comienza con dos nodos conectados y funcionan en dos switches de clúster Nexus 5596.
- El switch del clúster CL2 debe ser sustituido por C2 ([Pasos 1 - 19](#))
 - El tráfico de todos los puertos del clúster y las LIF de todos los nodos conectados a CL2 se migran a los primeros puertos del clúster y las LIF conectadas a CL1.
 - Desconecte el cableado de todos los puertos del clúster de todos los nodos conectados a CL2 y, a continuación, utilice un cableado de desconexión compatible para volver a conectar los puertos al nuevo switch de clúster C2.
 - Desconecte el cableado entre los puertos ISL entre CL1 y CL2 y, a continuación, utilice el cableado de desconexión admitido para volver a conectar los puertos de CL1 a C2.
 - Se revierte el tráfico en todos los puertos del clúster y los LIF conectados a C2 en todos los nodos.
- El switch del clúster CL2 se debe sustituir por C2
 - El tráfico de todos los puertos de clúster o las LIF de todos los nodos conectados a CL1 se migran a los segundos puertos de clúster o las LIF conectadas a C2.
 - Desconecte el cableado de todos los puertos del clúster de todos los nodos conectados a CL1 y vuelva a conectarlo, mediante el cableado de desconexión compatible, al nuevo switch del clúster C1.
 - Desconecte el cableado entre los puertos ISL entre CL1 y C2 y vuelva a conectarse mediante el

cableado compatible, de C1 a C2.

- Se revierte el tráfico en todos los puertos del clúster o LIF conectados a C1 en todos los nodos.
- Se han añadido dos nodos FAS9000 al clúster con ejemplos que muestran los detalles del clúster.

Paso 1: Prepararse para la sustitución

Para sustituir un switch de clúster Nexus 5596 existente por un switch de clúster Nexus 3132Q-V, debe realizar una secuencia específica de tareas.

1. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=xh`

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



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

2. Muestra información sobre los dispositivos de la configuración:

```
network device-discovery show
```

Muestra el ejemplo

En el ejemplo siguiente se muestra cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster:

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	CL1	Ethernet1/1	N5K-C5596UP
	e0b	CL2	Ethernet1/1	N5K-C5596UP
	e0c	CL2	Ethernet1/2	N5K-C5596UP
	e0d	CL1	Ethernet1/2	N5K-C5596UP
n2	/cdp			
	e0a	CL1	Ethernet1/3	N5K-C5596UP
	e0b	CL2	Ethernet1/3	N5K-C5596UP
	e0c	CL2	Ethernet1/4	N5K-C5596UP
	e0d	CL1	Ethernet1/4	N5K-C5596UP

8 entries were displayed.

3. Determine el estado administrativo u operativo de cada interfaz de clúster:

- a. Mostrar los atributos del puerto de red:

```
network port show
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los atributos de puerto de red en un sistema:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

a. Mostrar información acerca de las interfaces lógicas:

```
network interface show
```

Muestra el ejemplo

En el ejemplo siguiente se muestra la información general acerca de todas las LIF de su sistema:

```
cluster::*> network interface show -role cluster
(network interface show)

      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
e0a      true      n1_clus1      up/up      10.10.0.1/24      n1
e0b      true      n1_clus2      up/up      10.10.0.2/24      n1
e0c      true      n1_clus3      up/up      10.10.0.3/24      n1
e0d      true      n1_clus4      up/up      10.10.0.4/24      n1
e0a      true      n2_clus1      up/up      10.10.0.5/24      n2
e0b      true      n2_clus2      up/up      10.10.0.6/24      n2
e0c      true      n2_clus3      up/up      10.10.0.7/24      n2
e0d      true      n2_clus4      up/up      10.10.0.8/24      n2
8 entries were displayed.
```

b. Muestra información acerca de los switches del clúster detectados:

```
system cluster-switch show
```

Muestra el ejemplo

En el siguiente ejemplo se muestran los switches de clúster que conoce el clúster, junto con sus direcciones IP de administración:

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX5596	cluster-network	10.10.1.101
Serial Number: 01234567		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.1(1)N1(1)		
Version Source: CDP		
CL2 NX5596	cluster-network	10.10.1.102
Serial Number: 01234568		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.1(1)N1(1)		
Version Source: CDP		

2 entries were displayed.

4. Ajuste la `-auto-revert` parámetro a. `false` En las LIF de cluster `clus1` y `clus2` en ambos nodos:

```
network interface modify
```

Muestra el ejemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```

5. Compruebe que el RCF y la imagen adecuados están instalados en los nuevos conmutadores 3132Q-V según sea necesario para sus requisitos y realice las personalizaciones esenciales del sitio, como usuarios y contraseñas, direcciones de red, etc.

Debe preparar ambos switches en este momento. Si necesita actualizar el RCF y la imagen, siga estos pasos:

- a. Vaya a la ["Switches Ethernet de Cisco"](#) En el sitio de soporte de NetApp.
- b. Anote el conmutador y las versiones de software necesarias en la tabla de esa página.
- c. Descargue la versión adecuada del RCF.
- d. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.
- e. Descargue la versión adecuada del software Image.

Consulte la página *ONTAP 8.x o posterior referencia de switches de red de administración y clúster Archivos de configuración*Download y, a continuación, haga clic en la versión adecuada.

Para encontrar la versión correcta, consulte la *ONTAP 8.x o posterior página de descarga del conmutador de red de clúster*.

6. Migre los LIF asociados con el segundo switch Nexus 5596 que se va a reemplazar:

```
network interface migrate
```

Muestra el ejemplo

El siguiente ejemplo muestra n1 y n2, pero la migración de LIF debe realizarse en todos los nodos:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -
destination-node n2 -destination-port e0d
```

7. Compruebe el estado del clúster:

```
network interface show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el resultado del anterior `network interface migrate` comando:

```
cluster::*> network interface show -role cluster
(network interface show)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e0a n1_clus1 up/up 10.10.0.1/24 n1
true
e0a n1_clus2 up/up 10.10.0.2/24 n1
false
e0d n1_clus3 up/up 10.10.0.3/24 n1
false
e0d n1_clus4 up/up 10.10.0.4/24 n1
true
e0a n2_clus1 up/up 10.10.0.5/24 n2
true
e0a n2_clus2 up/up 10.10.0.6/24 n2
false
e0d n2_clus3 up/up 10.10.0.7/24 n2
false
e0d n2_clus4 up/up 10.10.0.8/24 n2
true
8 entries were displayed.
```

8. Apague los puertos de interconexión de clúster que estén conectados físicamente al switch CL2:

```
network port modify
```

Muestra el ejemplo

Los siguientes comandos apagan los puertos especificados en n1 y n2, pero los puertos deben estar apagados en todos los nodos:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

9. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster
```


Muestra el ejemplo

En el ejemplo siguiente se muestra cómo hacer ping a las interfaces de clúster remoto:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

10. Apague los puertos ISL 41 a 48 en el switch activo Nexus 5596 CL1:

Muestra el ejemplo

En el siguiente ejemplo, se muestra cómo apagar los puertos ISL 41 a 48 en el switch Nexus 5596 CL1:

```
(CL1)# configure
(CL1) (Config)# interface e1/41-48
(CL1) (config-if-range)# shutdown
(CL1) (config-if-range)# exit
(CL1) (Config)# exit
(CL1) #
```

Si va a sustituir un Nexus 5010 o 5020, especifique los números de puerto adecuados para ISL.

11. Cree un ISL temporal entre CL1 y C2.

Muestra el ejemplo

En el siguiente ejemplo, se muestra una configuración de ISL temporal entre CL1 y C2:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

Paso 2: Configurar puertos

1. En todos los nodos, quite todos los cables conectados al switch CL2 Nexus 5596.

Con el cableado compatible, vuelva a conectar los puertos desconectados de todos los nodos al switch C2 Nexus 3132Q-V.

2. Retire todos los cables del conmutador Nexus 5596 CL2.

Conecte los cables de interrupción Cisco QSFP a SFP+ adecuados que conectan el puerto 1/24 del nuevo switch Cisco 3132Q-V, C2, a los puertos 45 a 48 en Nexus 5596, CL1 existente.

3. Compruebe que las interfaces eth1/45-48 ya tienen channel-group 1 mode active en su configuración en ejecución.
4. Traiga los puertos ISL 45 a 48 en el switch CL1 de Nexus 5596 activo.

Muestra el ejemplo

El ejemplo siguiente muestra los puertos ISL 45 a 48 que se están poniendo en marcha:

```
(CL1)# configure
(CL1)(Config)# interface e1/45-48
(CL1)(config-if-range)# no shutdown
(CL1)(config-if-range)# exit
(CL1)(Config)# exit
(CL1)#
```

5. Compruebe que los ISL son up En el interruptor Nexus 5596 CL1:

```
show port-channel summary
```

Muestra el ejemplo

Los puertos eth1/45 a eth1/48 deben indicar (P) con el significado de los puertos ISL up en el puerto-canal:

Example

```
CL1# 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
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type   Protocol  Member Ports
      Channel
-----
-----
1      Po1 (SU)      Eth     LACP      Eth1/41 (D)  Eth1/42 (D)
Eth1/43 (D)
                                   Eth1/44 (D)  Eth1/45 (P)
Eth1/46 (P)
                                   Eth1/47 (P)  Eth1/48 (P)
```

6. Compruebe que los ISL son up En el interruptor C2 3132Q-V:

```
show port-channel summary
```

Muestra el ejemplo

Los puertos eth1/24/1, eth1/24/2, eth1/24/3 y eth1/24/4 deben indicar (P) lo que significa que los puertos ISL se encuentran up en el puerto-canal:

```
C2# 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
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met

-----
-----
Group Port-          Type  Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth    LACP      Eth1/31 (D)  Eth1/32 (D)
2      Po2 (SU)       Eth    LACP      Eth1/24/1 (P) Eth1/24/2 (P)
Eth1/24/3 (P)
                                   Eth1/24/4 (P)
```

7. En todos los nodos, active todos los puertos de interconexión del clúster conectados al switch 3132Q-V C2:

```
network port modify
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran los puertos especificados que se están up en los nodos n1 y n2:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

8. En todos los nodos, revierte todos los LIF de interconexión del clúster migrados conectados a C2:

```
network interface revert
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los LIF de clúster migrados que se están volviendo a sus puertos principales en los nodos n1 y n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

9. Verifique que todos los puertos de interconexión de clúster ahora se reviertan a su origen:

```
network interface show
```

Muestra el ejemplo

En el ejemplo siguiente se muestra que las LIF en clus2 se han revertido a sus puertos raíz y se muestra que las LIF se han revertido correctamente si los puertos de la columna de puerto actual tienen el estado de `true` en la `Is Home` columna. Si la `Is Home` el valor es `false`, El LIF no se ha revertido.

```
cluster::*> network interface show -role cluster
(network interface show)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e0a n1_clus1 up/up 10.10.0.1/24 n1
true
e0b n1_clus2 up/up 10.10.0.2/24 n1
true
e0c n1_clus3 up/up 10.10.0.3/24 n1
true
e0d n1_clus4 up/up 10.10.0.4/24 n1
true
e0a n2_clus1 up/up 10.10.0.5/24 n2
true
e0b n2_clus2 up/up 10.10.0.6/24 n2
true
e0c n2_clus3 up/up 10.10.0.7/24 n2
true
e0d n2_clus4 up/up 10.10.0.8/24 n2
true
8 entries were displayed.
```

10. Compruebe que los puertos del clúster están conectados:

```
network port show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el resultado del anterior `network port modify` comando, comprobando que todas las interconexiones del clúster lo son up:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a      Cluster      Cluster      up    9000  auto/10000  -
-
e0b      Cluster      Cluster      up    9000  auto/10000  -
-
e0c      Cluster      Cluster      up    9000  auto/10000  -
-
e0d      Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a      Cluster      Cluster      up    9000  auto/10000  -
-
e0b      Cluster      Cluster      up    9000  auto/10000  -
-
e0c      Cluster      Cluster      up    9000  auto/10000  -
-
e0d      Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

11. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster
```


Muestra el ejemplo

En el ejemplo siguiente se muestra cómo hacer ping a las interfaces de clúster remoto:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

12. En cada nodo del clúster, migre las interfaces asociadas con el primer switch Nexus 5596, CL1, que se sustituirá:

```
network interface migrate
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos o las LIF que se están migrando en los nodos n1 y n2:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-source-node n1 -
destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-source-node n1 -
destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-source-node n2 -
destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-source-node n2 -
destination-node n2 -destination-port e0c
```

13. Compruebe el estado del clúster:

```
network interface show
```

Muestra el ejemplo

El siguiente ejemplo muestra que las LIF de clúster necesarias se han migrado a puertos de clúster adecuados alojados en el switch de clúster C2:

```
(network interface show)

Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e0b n1_clus1 up/up 10.10.0.1/24 n1
false
e0b n1_clus2 up/up 10.10.0.2/24 n1
true
e0c n1_clus3 up/up 10.10.0.3/24 n1
true
e0c n1_clus4 up/up 10.10.0.4/24 n1
false
e0b n2_clus1 up/up 10.10.0.5/24 n2
false
e0b n2_clus2 up/up 10.10.0.6/24 n2
true
e0c n2_clus3 up/up 10.10.0.7/24 n2
true
e0c n2_clus4 up/up 10.10.0.8/24 n2
false
8 entries were displayed.

-----
```

14. En todos los nodos, apague los puertos de nodo que estén conectados a CL1:

```
network port modify
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos especificados que se están apagando en los nodos n1 y n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

15. Apague los puertos ISL 24, 31 y 32 en el interruptor C2 activo 3132Q-V:

shutdown

Muestra el ejemplo

El ejemplo siguiente muestra cómo cerrar ISL 24, 31 y 32:

```
C2# configure
C2(Config)# interface e1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if)# exit
C2#
```

16. En todos los nodos, quite todos los cables conectados al switch CL1 Nexus 5596.

Con el cableado compatible, vuelva a conectar los puertos desconectados de todos los nodos al switch Nexus 3132Q-V C1.

17. Retire el cable de arranque QSFP de los puertos Nexus 3132Q-V C2 e1/24.

Conecte los puertos e1/31 y e1/32 en C1 a los puertos e1/31 y e1/32 en C2 utilizando cables de fibra óptica Cisco QSFP o de conexión directa compatibles.

18. Restaure la configuración en el puerto 24 y retire el canal de puerto temporal 2 en C2:

```

C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[#####] 100%
Copy Complete.

```

19. Conecte los puertos ISL 31 y 32 en C2, el switch activo 3132Q-V: no shutdown

Muestra el ejemplo

El ejemplo siguiente muestra cómo instalar ISL 31 y 32 en el switch 3132Q-V C2:

```

C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[#####] 100%
Copy Complete.

```

Paso 3: Verificar la configuración

1. Compruebe que las conexiones ISL están up En el interruptor C2 3132Q-V:

```
show port-channel summary
```

Muestra el ejemplo

Los puertos eth1/31 y eth1/32 deben indicar (P) , Lo que significa que ambos puertos ISL son up en el puerto-canal:

```
C1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      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)
```

2. En todos los nodos, traiga todos los puertos de interconexión del clúster conectados al nuevo switch C1 de 3132Q-V:

```
network port modify
```

Muestra el ejemplo

En el siguiente ejemplo se muestran todos los puertos de interconexión de clúster que se están creando para n1 y n2 en el switch C1 de 3132Q-V:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

3. Compruebe el estado del puerto del nodo del clúster:

```
network port show
```

Muestra el ejemplo

En el siguiente ejemplo se comprueba que todos los puertos de interconexión de clúster de todos los nodos del nuevo switch C1 de 3132Q-V. up:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

4. En todos los nodos, revierte los LIF de clúster específicos a sus puertos de inicio:

```
network interface revert
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los LIF de clúster específicos que se están reteniendo a sus puertos raíz en los nodos n1 y n2:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

5. Compruebe que la interfaz es la principal:

```
network interface show
```


Muestra el ejemplo

En el ejemplo siguiente se muestra el estado de las interfaces de interconexión del clúster es up y..
Is home para n1 y n2:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0b      true
      n1_clus3      up/up      10.10.0.3/24      n1
e0c      true
      n1_clus4      up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1      up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2      up/up      10.10.0.6/24      n2
e0b      true
      n2_clus3      up/up      10.10.0.7/24      n2
e0c      true
      n2_clus4      up/up      10.10.0.8/24      n2
e0d      true
8 entries were displayed.
```

6. Haga ping a las interfaces remotas del clúster y, a continuación, realice una comprobación del servidor de llamadas de procedimiento remoto:

```
cluster ping-cluster
```

Muestra el ejemplo

En el ejemplo siguiente se muestra cómo hacer ping a las interfaces de clúster remoto:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

7. Expanda el clúster añadiendo nodos a los switches de clúster Nexus 3132Q-V.

8. Muestra la información sobre los dispositivos de la configuración:

- ° network device-discovery show
- ° network port show -role cluster
- ° network interface show -role cluster
- ° system cluster-switch show

Muestra el ejemplo

En los siguientes ejemplos se muestran los nodos n3 y n4 con puertos de clúster de 40 GbE conectados a los puertos e1/7 y e1/8, respectivamente en los dos switches de cluster Nexus 3132Q-V y ambos nodos se han Unido al cluster. Los puertos de interconexión de clúster de 40 GbE utilizados son e4a y e4e.

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-
C3132Q-V	e0b	C2	Ethernet1/1/1	N3K-
C3132Q-V	e0c	C2	Ethernet1/1/2	N3K-
C3132Q-V	e0d	C1	Ethernet1/1/2	N3K-
C3132Q-V				
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-
C3132Q-V	e0b	C2	Ethernet1/1/3	N3K-
C3132Q-V	e0c	C2	Ethernet1/1/4	N3K-
C3132Q-V	e0d	C1	Ethernet1/1/4	N3K-
C3132Q-V				
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-
C3132Q-V	e4e	C2	Ethernet1/7	N3K-
C3132Q-V				
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-
C3132Q-V	e4e	C2	Ethernet1/8	N3K-
C3132Q-V				

12 entries were displayed.

```
cluster::*> network port show -role cluster
(network port show)
Node: n1
```

Ignore

						Speed (Mbps)	
Health Port Status	Health IPspace Status	Broadcast	Domain	Link	MTU	Admin/Oper	
-----	-----	-----	-----	----	-----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

Node: n2

Ignore

						Speed (Mbps)	
Health Port Status	Health IPspace Status	Broadcast	Domain	Link	MTU	Admin/Oper	
-----	-----	-----	-----	----	-----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

Node: n3

Ignore

						Speed (Mbps)	
Health Port Status	Health IPspace Status	Broadcast	Domain	Link	MTU	Admin/Oper	
-----	-----	-----	-----	----	-----	-----	
-----	-----						
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							

```

e4e      Cluster      Cluster      up    9000 auto/40000 -
-

Node: n4

Ignore

Speed (Mbps)

Health    Health
Port      IPspace    Broadcast Domain Link MTU  Admin/Oper
Status    Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000 -
-

e4e      Cluster      Cluster      up    9000 auto/40000 -
-

12 entries were displayed.

```

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

```
(network interface show)
```

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

Cluster					
		n1_clus1	up/up	10.10.0.1/24	n1
e0a	true				
		n1_clus2	up/up	10.10.0.2/24	n1
e0b	true				
		n1_clus3	up/up	10.10.0.3/24	n1
e0c	true				
		n1_clus4	up/up	10.10.0.4/24	n1
e0d	true				
		n2_clus1	up/up	10.10.0.5/24	n2
e0a	true				
		n2_clus2	up/up	10.10.0.6/24	n2
e0b	true				
		n2_clus3	up/up	10.10.0.7/24	n2
e0c	true				
		n2_clus4	up/up	10.10.0.8/24	n2
e0d	true				
		n3_clus1	up/up	10.10.0.9/24	n3
e4a	true				
		n3_clus2	up/up	10.10.0.10/24	n3
e4e	true				
		n4_clus1	up/up	10.10.0.11/24	n4
e4a	true				
		n4_clus2	up/up	10.10.0.12/24	n4
e4e	true				

```
12 entries were displayed.
```

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
CL1 NX5596	cluster-network	10.10.1.101
Serial Number: 01234567		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.1(1)N1(1)		
Version Source: CDP		
CL2 NX5596	cluster-network	10.10.1.102
Serial Number: 01234568		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.1(1)N1(1)		
Version Source: CDP		

4 entries were displayed.

9. Retire el Nexus 5596 sustituido si no se quitan automáticamente:

```
system cluster-switch delete
```

Muestra el ejemplo

El siguiente ejemplo muestra cómo quitar el Nexus 5596:

```
cluster::> system cluster-switch delete -device CL1  
cluster::> system cluster-switch delete -device CL2
```

10. Configure los clústeres clus1 y clus2 para revertir automáticamente cada nodo y confirmar.

Muestra el ejemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto  
-revert true  
cluster::*> network interface modify -vserver node1 -lif clus2 -auto  
-revert true  
cluster::*> network interface modify -vserver node2 -lif clus1 -auto  
-revert true  
cluster::*> network interface modify -vserver node2 -lif clus2 -auto  
-revert true
```

11. Compruebe que se supervisan los switches de clúster adecuados:

```
system cluster-switch show
```

Muestra el ejemplo

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

12. Habilite la función de recogida de registro de supervisión del estado del switch para recopilar archivos de registro relacionados con el switch:

```
system cluster-switch log setup-password
```

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

Muestra el ejemplo

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

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

Enter the switch name: C1
**RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

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

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

Enabling cluster switch log collection.

cluster::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

13. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

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

Migre de los switches de clúster CN1610 a los switches de clúster Cisco Nexus 3132Q-V.

Siga este procedimiento para sustituir los switches de clúster CN1610 existentes por switches de clúster Cisco Nexus 3132Q-V.

Revise los requisitos

Revise los requisitos del CN1610 de NetApp en ["Requisitos para sustituir los switches de clúster Cisco Nexus 3132Q-V."](#).

Para obtener más información, consulte:

- ["Página de descripción de NetApp CN1601 y CN1610"](#)
- ["Página de descripción de Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Sustituya el interruptor

Nomenclatura de switch y nodo

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

- Los resultados del comando pueden variar en función de las diferentes versiones del software ONTAP.
- Los interruptores CN1610 que se deben sustituir son CL1 y CL2.
- Los switches Nexus 3132Q-V que sustituyen a los switches CN1610 son C1 y C2.
- n1_clus1 es la primera interfaz lógica del clúster (LIF) conectada al switch del clúster 1 (CL1 o C1) para el nodo n1.
- n1_clus2 es la primera LIF del clúster que está conectada al switch de clúster 2 (CL2 o C2) para el nodo n1.
- n1_clus3 es la segunda LIF conectada al switch de clúster 2 (CL2 o C2) para el nodo n1.
- n1_clus4 es la segunda LIF conectada al switch de clúster 1 (CL1 o C1) para el nodo n1.
- Los nodos son n1, n2, n3 y n4.
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) página.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan cuatro nodos:

- Dos nodos utilizan cuatro puertos de interconexión de clúster de 10 GbE: E0a, e0b, e0c y e0d.
- Los otros dos nodos utilizan dos cables de fibra de interconexión de clúster de 40/100 GbE: e4a y e4e.

La ["Hardware Universe"](#) tiene información acerca de los cables de fibra de clúster en las plataformas.

Acerca de esta tarea

Este procedimiento cubre el siguiente caso:

- El clúster comienza con dos nodos conectados a dos switches de clúster CN1610.
- El switch del clúster CL2 se debe sustituir por C2

- El tráfico de todos los puertos del clúster y las LIF de todos los nodos conectados a CL2 se migran a los primeros puertos del clúster y las LIF conectadas a CL1.
- Desconecte el cableado de todos los puertos de clúster de todos los nodos conectados a CL2 y, a continuación, utilice cableado de arranque compatible para volver a conectar los puertos al nuevo switch de clúster C2.
- Desconecte el cableado entre los puertos ISL CL1 y CL2 y, a continuación, utilice un cableado de arranque compatible para volver a conectar los puertos de CL1 a C2.
- Se revierte el tráfico en todos los puertos del clúster y los LIF conectados a C2 en todos los nodos.
- El interruptor del grupo CL1 se debe sustituir por C1
 - El tráfico de todos los puertos de clúster y las LIF de todos los nodos conectados a CL1 se migran a los segundos puertos de clúster y las LIF conectadas a C2.
 - Desconecte el cableado de todos los puertos del clúster de todos los nodos conectados a CL1 y, a continuación, utilice el cableado de arranque compatible para volver a conectar los puertos al nuevo switch del clúster C1.
 - Desconecte el cableado entre los puertos ISL CL1 y C2 y utilice un cableado de arranque compatible para volver a conectar los puertos de C1 a C2.
 - Se revierte el tráfico en todos los puertos de clúster migrados y LIF conectados a C1 en todos los nodos.



Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

Paso 1: Prepararse para la sustitución

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

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

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



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

2. Muestra información sobre los dispositivos de la configuración:

```
network device-discovery show
```

Muestra el ejemplo

El ejemplo siguiente muestra cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster:

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	CL1	0/1	CN1610
	e0b	CL2	0/1	CN1610
	e0c	CL2	0/2	CN1610
	e0d	CL1	0/2	CN1610
n2	/cdp			
	e0a	CL1	0/3	CN1610
	e0b	CL2	0/3	CN1610
	e0c	CL2	0/4	CN1610
	e0d	CL1	0/4	CN1610

8 entries were displayed.

3. Determinar el estado administrativo u operativo de cada interfaz de clúster.

a. Muestre los atributos de puerto de red del clúster:

```
network port show
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los atributos de puerto de red en un sistema:

```
cluster::*> network port show -role Cluster
(network port show)

Node: n1

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status                                     Status Health
-----
e0a   cluster  cluster   up    9000  auto/10000    -       -
e0b   cluster  cluster   up    9000  auto/10000    -       -
e0c   cluster  cluster   up    9000  auto/10000    -       -
e0d   cluster  cluster   up    9000  auto/10000    -       -

Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status                                     Status Health
-----
e0a   cluster  cluster   up    9000  auto/10000    -       -
e0b   cluster  cluster   up    9000  auto/10000    -       -
e0c   cluster  cluster   up    9000  auto/10000    -       -
e0d   cluster  cluster   up    9000  auto/10000    -       -

8 entries were displayed.
```

b. Mostrar información acerca de las interfaces lógicas:

```
network interface show
```

Muestra el ejemplo

En el ejemplo siguiente se muestra la información general acerca de todas las LIF de su sistema:

```
cluster::*> network interface show -role Cluster
(network interface show)
```

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

Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true					
	n1_clus2	up/up	10.10.0.2/24	n1	e0b
true					
	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true					
	n1_clus4	up/up	10.10.0.4/24	n1	e0d
true					
	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true					
	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true					
	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true					
	n2_clus4	up/up	10.10.0.8/24	n2	e0d
true					

8 entries were displayed.

c. Muestra información sobre los switches del clúster detectados:

```
system cluster-switch show
```


Muestra el ejemplo

En el siguiente ejemplo se muestran los switches de clúster que conoce el clúster, junto con sus direcciones IP de administración:

```
cluster::> system cluster-switch show
```

Switch	Type	Address	Model
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			

2 entries were displayed.

4. Ajuste la `-auto-revert` Parámetro a `FALSE` en las LIF del clúster `clus1` y `clus4` en ambos nodos:

```
network interface modify
```

Muestra el ejemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto  
-revert false  
cluster::*> network interface modify -vserver node1 -lif clus4 -auto  
-revert false  
cluster::*> network interface modify -vserver node2 -lif clus1 -auto  
-revert false  
cluster::*> network interface modify -vserver node2 -lif clus4 -auto  
-revert false
```

5. Compruebe que el RCF y la imagen adecuados están instalados en los nuevos conmutadores 3132Q-V según sea necesario para sus requisitos y realice las personalizaciones esenciales del sitio, como usuarios y contraseñas, direcciones de red, etc.

Debe preparar ambos switches en este momento. Si necesita actualizar el RCF y la imagen, siga estos pasos:

- a. Consulte "[Switches Ethernet de Cisco](#)" En el sitio de soporte de NetApp.
- b. Anote el conmutador y las versiones de software necesarias en la tabla de esa página.
- c. Descargue la versión adecuada del RCF.
- d. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.
- e. Descargue la versión adecuada del software Image.

["Descarga del archivo de configuración de referencia del conmutador de red de administración y clúster Cisco®"](#)

6. Migre los LIF asociados con el segundo switch CN1610 que se va a reemplazar:

```
network interface migrate
```



Debe migrar los LIF del clúster desde una conexión al nodo, ya sea a través del procesador de servicio o de la interfaz de gestión de nodos, que posee la LIF de clúster que se está migrando.

Muestra el ejemplo

El siguiente ejemplo muestra n1 y n2, pero la migración de LIF debe realizarse en todos los nodos:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-destination-node n2 -destination-port e0d
```

7. Compruebe el estado del clúster:

```
network interface show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el resultado del anterior `network interface migrate` comando:

```
cluster::*> network interface show -role Cluster
(network interface show)
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----	-----	-----	-----	-----	-----	-----
Cluster						
true	n1_clus1	up/up	10.10.0.1/24	n1	e0a	
false	n1_clus2	up/up	10.10.0.2/24	n1	e0a	
false	n1_clus3	up/up	10.10.0.3/24	n1	e0d	
true	n1_clus4	up/up	10.10.0.4/24	n1	e0d	
true	n2_clus1	up/up	10.10.0.5/24	n2	e0a	
false	n2_clus2	up/up	10.10.0.6/24	n2	e0a	
false	n2_clus3	up/up	10.10.0.7/24	n2	e0d	
true	n2_clus4	up/up	10.10.0.8/24	n2	e0d	

8 entries were displayed.

8. Apague los puertos de interconexión de clúster que estén conectados físicamente al switch CL2:

```
network port modify
```

Muestra el ejemplo

Los siguientes comandos apagan los puertos especificados en n1 y n2, pero los puertos deben estar apagados en todos los nodos:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

9. Haga ping a las interfaces remotas del clúster y, a continuación, realice una comprobación del servidor de llamadas de procedimiento remoto:

```
cluster ping-cluster
```

Muestra el ejemplo

En el ejemplo siguiente se muestra cómo hacer ping a las interfaces de clúster remoto:

```

cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)

```

10. Apague los puertos ISL 13 a 16 en el switch CN1610 activo CL1:

shutdown

Muestra el ejemplo

En el siguiente ejemplo, se muestra cómo apagar los puertos ISL 13 a 16 en el switch CN1610 CL1:

```
(CL1)# configure
(CL1)(Config)# interface 0/13-0/16
(CL1)(Interface 0/13-0/16)# shutdown
(CL1)(Interface 0/13-0/16)# exit
(CL1)(Config)# exit
(CL1)#
```

11. Cree un ISL temporal entre CL1 y C2:

Muestra el ejemplo

En el siguiente ejemplo se crea un ISL temporal entre CL1 (puertos 13-16) y C2 (puertos e1/24/1-4):

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

Paso 2: Configurar puertos

1. En todos los nodos, quite los cables conectados al conmutador CL2 CN1610.

Con el cableado compatible, debe volver a conectar los puertos desconectados de todos los nodos al switch C2 de Nexus 3132Q-V.

2. Quite cuatro cables ISL de los puertos 13 a 16 en el conmutador CL1 CN1610.

Debe conectar los cables de conexión entre Cisco QSFP a SFP+ del puerto 1/24 del nuevo switch C2 de Cisco 3132Q-V, a los puertos 13 a 16 del switch CL1 existente del CN1610.



Al volver a conectar los cables al nuevo switch Cisco 3132Q-V, debe utilizar cables de fibra óptica o conductores twinax de Cisco.

3. Para que el ISL sea dinámico, configure la interfaz ISL 3/1 en el switch CN1610 activo para deshabilitar el modo estático: `no port-channel static`

Esta configuración coincide con la configuración ISL en el switch 3132Q-V C2 cuando se configuran los ISL en ambos switches en el paso 11

Muestra el ejemplo

En el ejemplo siguiente se muestra la configuración de la interfaz ISL 3/1 mediante `no port-channel static` Comando para que el ISL sea dinámico:

```
(CL1)# configure
(CL1)(Config)# interface 3/1
(CL1)(Interface 3/1)# no port-channel static
(CL1)(Interface 3/1)# exit
(CL1)(Config)# exit
(CL1)#
```

4. Traiga ISL 13 a 16 en el conmutador CL1 CN1610 activo.

Muestra el ejemplo

En el siguiente ejemplo se muestra el proceso de puesta en marcha de los puertos ISL 13 a 16 en la interfaz puerto-canal 3/1:

```
(CL1)# configure
(CL1)(Config)# interface 0/13-0/16,3/1
(CL1)(Interface 0/13-0/16,3/1)# no shutdown
(CL1)(Interface 0/13-0/16,3/1)# exit
(CL1)(Config)# exit
(CL1)#
```

5. Compruebe que los ISL son up En el conmutador CN1610 CL1:

```
show port-channel
```

El "Estado de enlace" debe ser Up, "Tipo" debe ser Dynamic, Y la columna "Puerto activo" debe ser True para los puertos 0/13 a 0/16:

Muestra el ejemplo

```
(CL1)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr Ports	Device/ Timeout	Port Speed	Port Active
-----	-----	-----	-----
0/13	actor/long partner/long	10 Gb Full	True
0/14	actor/long partner/long	10 Gb Full	True
0/15	actor/long partner/long	10 Gb Full	True
0/16	actor/long partner/long	10 Gb Full	True

6. Compruebe que los ISL son up En el interruptor C2 3132Q-V:

```
show port-channel summary
```

Muestra el ejemplo

Los puertos eth1/24/1 a eth1/24/4 deben indicarse (P) , Lo que significa que los cuatro puertos ISL están activos en el puerto-canal. Debe indicar eth1/31 y eth1/32 (D) puesto que no están conectados:

```
C2# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
      Channel
-----
-----
1      Po1 (SU)       Eth       LACP      Eth1/31 (D)  Eth1/32 (D)
2      Po2 (SU)       Eth       LACP      Eth1/24/1 (P) Eth1/24/2 (P)
Eth1/24/3 (P)
                                   Eth1/24/4 (P)
```

7. Ponga en funcionamiento todos los puertos de interconexión del clúster que están conectados al switch C2 3132Q-V en todos los nodos:

```
network port modify
```

Muestra el ejemplo

El siguiente ejemplo muestra cómo activar los puertos de interconexión del clúster conectados al switch C2 3132Q-V:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

8. Revierte todos los LIF de interconexión del clúster migrados que están conectados a C2 en todos los nodos:

```
network interface revert
```

Muestra el ejemplo

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

9. Compruebe que todos los puertos de interconexión de clúster se hayan revertido a sus puertos principales:

```
network interface show
```

Muestra el ejemplo

En el ejemplo siguiente se muestra que las LIF de clus2 se revierten a sus puertos raíz, y se muestra que las LIF se revierten correctamente si el estado de los puertos de la columna "puerto actual" es de true En la columna "es de inicio". Si el valor es Home false, Entonces el LIF no se revierte.

```
cluster::*> network interface show -role cluster
(network interface show)
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Cluster	n1_clus1	up/up	10.10.0.1/24	n1	e0a	true
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	true
	n2_clus1	up/up	10.10.0.5/24	n2	e0a	true
	n2_clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2_clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2_clus4	up/up	10.10.0.8/24	n2	e0d	true

8 entries were displayed.

10. Compruebe que todos los puertos del clúster estén conectados:

```
network port show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el resultado del anterior `network port modify` comando, comprobando que todas las interconexiones del clúster lo son up:

```
cluster::*> network port show -role Cluster
(network port show)

Node: n1

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Domain                                     Admin/Open  Status  Health
-----  -
e0a    cluster  cluster    up    9000  auto/10000    -       -
e0b    cluster  cluster    up    9000  auto/10000    -       -
e0c    cluster  cluster    up    9000  auto/10000    -       -
e0d    cluster  cluster    up    9000  auto/10000    -       -

Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Domain                                     Admin/Open  Status  Health
-----  -
e0a    cluster  cluster    up    9000  auto/10000    -       -
e0b    cluster  cluster    up    9000  auto/10000    -       -
e0c    cluster  cluster    up    9000  auto/10000    -       -
e0d    cluster  cluster    up    9000  auto/10000    -       -

8 entries were displayed.
```

11. Haga ping a las interfaces remotas del clúster y, a continuación, realice una comprobación del servidor de llamadas de procedimiento remoto:

```
cluster ping-cluster
```

Muestra el ejemplo

En el ejemplo siguiente se muestra cómo hacer ping a las interfaces de clúster remoto:

```

cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)

```

12. En cada nodo del clúster, migre las interfaces asociadas al primer switch CL1 CN1610 que se sustituirá:

```
network interface migrate
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos o las LIF que se están migrando en los nodos n1 y n2:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-destination-node n2 -destination-port e0c
```

13. Compruebe el estado del clúster:

```
network interface show
```


Muestra el ejemplo

El siguiente ejemplo muestra que las LIF de clúster necesarias se han migrado a los puertos de clúster correspondientes alojados en el switch de clúster C2:

```
cluster::*> network interface show -role Cluster
(network interface show)
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----	-----	-----	-----	-----	-----	-----
Cluster						
false	n1_clus1	up/up	10.10.0.1/24	n1	e0b	
true	n1_clus2	up/up	10.10.0.2/24	n1	e0b	
true	n1_clus3	up/up	10.10.0.3/24	n1	e0c	
false	n1_clus4	up/up	10.10.0.4/24	n1	e0c	
false	n2_clus1	up/up	10.10.0.5/24	n2	e0b	
true	n2_clus2	up/up	10.10.0.6/24	n2	e0b	
true	n2_clus3	up/up	10.10.0.7/24	n2	e0c	
false	n2_clus4	up/up	10.10.0.8/24	n2	e0c	

8 entries were displayed.

14. Apague los puertos de nodo que estén conectados a CL1 en todos los nodos:

```
network port modify
```

Muestra el ejemplo

En el ejemplo siguiente se muestra cómo apagar los puertos especificados en los nodos n1 y n2:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

15. Apague los puertos ISL 24, 31 y 32 en el interruptor C2 activo 3132Q-V:

shutdown

Muestra el ejemplo

El ejemplo siguiente muestra cómo apagar los ISL 24, 31 y 32 en el conmutador C2 3132Q-V activo:

```
C2# configure
C2(config)# interface ethernet 1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
C2#
```

16. Quite los cables conectados al conmutador CL1 CN1610 de todos los nodos.

Con el cableado compatible, debe volver a conectar los puertos desconectados de todos los nodos al conmutador C1 Nexus 3132Q-V.

17. Retire los cables QSFP del puerto nexus 3132Q-V C2 e1/24.

Debe conectar los puertos e1/31 y e1/32 en C1 a los puertos e1/31 y e1/32 en C2 utilizando cables de fibra óptica Cisco QSFP o de conexión directa.

18. Restaure la configuración en el puerto 24 y retire el canal de puerto temporal 2 en C2, copiando el `running-configuration` en la `startup-configuration` archivo.

Muestra el ejemplo

En el ejemplo siguiente se copia el running-configuration en la startup-configuration archivo:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# interface e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[#####] 100%
Copy Complete.
```

19. Conecte los puertos ISL 31 y 32 en C2, el switch activo 3132Q-V:

```
no shutdown
```

Muestra el ejemplo

El ejemplo siguiente muestra cómo instalar ISL 31 y 32 en el switch 3132Q-V C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[#####] 100%
Copy Complete.
```

Paso 3: Verificar la configuración

1. Compruebe que las conexiones ISL están up En el interruptor C2 3132Q-V:

```
show port-channel summary
```

Los puertos eth1/31 y eth1/32 deben indicar (P), Lo que significa que ambos puertos ISL son up en el puerto-canal.

Muestra el ejemplo

```
C1# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        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)
```

2. Conecte todos los puertos de interconexión del clúster conectados al nuevo switch 3132Q-V C1 en todos los nodos:

```
network port modify
```

Muestra el ejemplo

El siguiente ejemplo muestra cómo mostrar todos los puertos de interconexión del clúster conectados al nuevo switch C1 de 3132Q-V:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

3. Compruebe el estado del puerto del nodo del clúster:

```
network port show
```

Muestra el ejemplo

En el siguiente ejemplo se comprueba que todos los puertos de interconexión de clúster de n1 y n2 del nuevo switch C1 de 3132Q-V. up:

```
cluster::*> network port show -role Cluster
(network port show)

Node: n1

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Domain                               Admin/Open  Status  Health
-----
-----
e0a    cluster  cluster    up    9000  auto/10000    -       -
e0b    cluster  cluster    up    9000  auto/10000    -       -
e0c    cluster  cluster    up    9000  auto/10000    -       -
e0d    cluster  cluster    up    9000  auto/10000    -       -

Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Domain                               Admin/Open  Status  Health
-----
-----
e0a    cluster  cluster    up    9000  auto/10000    -       -
e0b    cluster  cluster    up    9000  auto/10000    -       -
e0c    cluster  cluster    up    9000  auto/10000    -       -
e0d    cluster  cluster    up    9000  auto/10000    -       -

8 entries were displayed.
```

4. Revierte todos los LIF de interconexión del clúster migrados que estaban conectados originalmente a C1 en todos los nodos:

```
network interface revert
```

Muestra el ejemplo

El ejemplo siguiente muestra cómo revertir las LIF del clúster migradas a sus puertos principales:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

5. Compruebe que la interfaz se encuentra ahora en casa:

```
network interface show
```

Muestra el ejemplo

En el ejemplo siguiente se muestra el estado de las interfaces de interconexión del clúster es up y..
Is home para n1 y n2:

```
cluster::*> network interface show -role Cluster
(network interface show)
```

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

Cluster						
	n1_clus1	up/up	10.10.0.1/24	n1	e0a	
true						
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	
true						
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	
true						
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	
true						
	n2_clus1	up/up	10.10.0.5/24	n2	e0a	
true						
	n2_clus2	up/up	10.10.0.6/24	n2	e0b	
true						
	n2_clus3	up/up	10.10.0.7/24	n2	e0c	
true						
	n2_clus4	up/up	10.10.0.8/24	n2	e0d	
true						

8 entries were displayed.

6. Haga ping a las interfaces remotas del clúster y, a continuación, realice una comprobación del servidor de llamadas de procedimiento remoto:

```
cluster ping-cluster
```

Muestra el ejemplo

En el ejemplo siguiente se muestra cómo hacer ping a las interfaces de clúster remoto:


```

cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)

```

7. Expanda el clúster añadiendo nodos a los switches de clúster Nexus 3132Q-V.

8. Muestra la información sobre los dispositivos de la configuración:

- `network device-discovery show`
- `network port show -role cluster`
- `network interface show -role cluster`
- `system cluster-switch show`

Muestra el ejemplo

En los siguientes ejemplos se muestran los nodos n3 y n4 con puertos de clúster de 40 GbE conectados a los puertos e1/7 y e1/8, respectivamente en los dos switches de cluster Nexus 3132Q-V y ambos nodos se han Unido al cluster. Los puertos de interconexión de clúster de 40 GbE utilizados son e4a y e4e.

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0d	C1	Ethernet1/1/2	N3K-C3132Q-V
	e0a	C1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/3	N3K-C3132Q-V
n3	/cdp			
	e0c	C2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/4	N3K-C3132Q-V
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
n4	/cdp			
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V

12 entries were displayed.

```
cluster::*> network port show -role cluster
(network port show)
```

Node: n1

		Broadcast		Speed (Mbps)		Health	
Ignore							
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	
Health	Status						

e0a	cluster	cluster	up	9000	auto/10000	-	-
e0b	cluster	cluster	up	9000	auto/10000	-	-
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n2

		Broadcast			Speed (Mbps)	Health	
Ignore							
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	
Health	Status						
-----	-----	-----	-----	-----	-----	-----	

e0a	cluster	cluster	up	9000	auto/10000	-	-
e0b	cluster	cluster	up	9000	auto/10000	-	-
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n3

		Broadcast			Speed (Mbps)	Health	
Ignore							
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	
Health	Status						
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e4a	cluster	cluster	up	9000	auto/40000	-	-
e4e	cluster	cluster	up	9000	auto/40000	-	-

Node: n4

		Broadcast			Speed (Mbps)	Health	
Ignore							
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	
Health	Status						
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e4a	cluster	cluster	up	9000	auto/40000	-	-
e4e	cluster	cluster	up	9000	auto/40000	-	-

12 entries were displayed.

```
cluster::*> network interface show -role Cluster
(network interface show)
```

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

Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true					
	n1_clus2	up/up	10.10.0.2/24	n1	e0b
true					
	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true					
	n1_clus4	up/up	10.10.0.4/24	n1	e0d
true					
	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true					
	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true					
	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true					
	n2_clus4	up/up	10.10.0.8/24	n2	e0d
true					
	n3_clus1	up/up	10.10.0.9/24	n3	e4a
true					
	n3_clus2	up/up	10.10.0.10/24	n3	e4e
true					
	n4_clus1	up/up	10.10.0.11/24	n4	e4a
true					
	n4_clus2	up/up	10.10.0.12/24	n4	e4e
true					

```
12 entries were displayed.
```

```
cluster::> system cluster-switch show
```

Switch	Type	Address	Model

C1	cluster-network	10.10.1.103	
NX3132V			
Serial Number: FOX000001			
Is Monitored: true			
Reason:			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
7.0(3)I4(1)			
Version Source: CDP			
C2	cluster-network	10.10.1.104	
NX3132V			
Serial Number: FOX000002			
Is Monitored: true			
Reason:			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
7.0(3)I4(1)			
Version Source: CDP			
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	
CN1610			
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			

4 entries were displayed.

9. Extraiga los interruptores CN1610 sustituidos si no se retiran automáticamente:

```
system cluster-switch delete
```

Muestra el ejemplo

El siguiente ejemplo muestra cómo quitar los switches CN1610:

```
cluster::> system cluster-switch delete -device CL1
cluster::> system cluster-switch delete -device CL2
```

10. Configure cluster clus1 y clus4 para `-auto-revert` en cada nodo y confirme:

Muestra el ejemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus4 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus4 -auto
-revert true
```

11. Compruebe que se supervisan los switches de clúster adecuados:

```
system cluster-switch show
```

Muestra el ejemplo

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

12. Habilite la función de recogida de registro de supervisión del estado del switch para recopilar archivos de registro relacionados con el switch:

```
system cluster-switch log setup-password
```

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


Muestra el ejemplo

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

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

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

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

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

Enabling cluster switch log collection.

cluster::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

13. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

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

Migre de un clúster sin switches a un clúster con switches de dos nodos

Si tiene un clúster sin switches de dos nodos, puede seguir este procedimiento para migrar a un clúster con switches de dos nodos que incluya switches de red de clúster Cisco Nexus 3132Q-V. El procedimiento de sustitución es un procedimiento no disruptivo (NDO).

Revise los requisitos

Conexiones de puertos y nodos

Asegúrese de comprender los requisitos de cableado y las conexiones de puertos y nodos cuando migre a un clúster con switches de dos nodos con switches de clúster Cisco Nexus 3132Q-V.

- Los switches de clúster utilizan los puertos de enlace entre switches (ISL) e1/31-32.
- La ["Hardware Universe"](#) Contiene información sobre el cableado compatible con los switches Nexus 3132Q-V:
 - Los nodos con conexiones de clúster de 10 GbE requieren módulos ópticos QSFP con cables de fibra de cable multiconector o cables de cobre QSFP a SFP+.
 - Los nodos con conexiones de clúster de 40/100 GbE requieren módulos ópticos QSFP/QSFP28 compatibles con cables de fibra o cables de conexión directa de cobre QSFP/QSFP28.
 - Los switches de clúster utilizan el cableado ISL adecuado: 2 cables de conexión directa de cobre o fibra QSFP28.
- En Nexus 3132Q-V, puede utilizar puertos QSFP como Ethernet de 40/100 GB o modos Ethernet de 4 x10 GB.

De forma predeterminada, hay 32 puertos en el modo Ethernet de 40/100 GB. Estos puertos Ethernet de 40 GB están numerados en una convención de nomenclatura de 2 tubos. Por ejemplo, el segundo puerto Ethernet de 40 GB está numerado como 1/2. El proceso de cambiar la configuración de Ethernet de 40 GB a Ethernet de 10 GB se denomina *breakout* y el proceso de cambiar la configuración de Ethernet de 10 GB a Ethernet de 40 GB se denomina *breakin*. Cuando se rompe un puerto Ethernet de 40/100 GB en puertos Ethernet de 10 GB, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tubos. Por ejemplo, los puertos de arranque del segundo puerto Ethernet de 40/100 GB están numerados como 1/2/1, 1/2/2, 1/2/3, 1/2/4.

- En el lado izquierdo de Nexus 3132Q-V se encuentra un conjunto de cuatro puertos SFP+ multiplexados al primer puerto QSFP.

De forma predeterminada, el RCF está estructurado para utilizar el primer puerto QSFP.

Puede hacer que cuatro puertos SFP+ estén activos en lugar de un puerto QSFP para Nexus 3132Q-V mediante el `hardware profile front portmode sfp-plus` comando. Del mismo modo, se puede restablecer Nexus 3132Q-V para utilizar un puerto QSFP en lugar de cuatro puertos SFP+ mediante el `hardware profile front portmode qsfp` comando.

- Asegúrese de configurar algunos de los puertos en Nexus 3132Q-V para que funcionen a 10 GbE o 40/100 GbE.

Puede extraer los primeros seis puertos en modo 4x10 GbE mediante el `interface breakout module 1 port 1-6 map 10g-4x` comando. De forma similar, puede volver a agrupar los primeros seis puertos

QSFP+ de la configuración de cable mediante el `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del switch de red de clúster de Cisco ®"](#) página.

Lo que necesitará

- Las configuraciones se configuran y funcionan correctamente.
- Los nodos que ejecutan ONTAP 9.4 o una versión posterior.
- Todos los puertos del clúster en `up` estado.
- Se admite el switch de clúster Cisco Nexus 3132Q-V.
- La configuración de red del clúster existente tiene:
 - La infraestructura de clúster Nexus 3132 es redundante y completamente funcional en ambos switches.
 - Las versiones más recientes de RCF y NX-OS en sus switches.

La ["Switches Ethernet de Cisco"](#) La página tiene información acerca de las versiones ONTAP y NX-OS que se admiten en este procedimiento.

- Conectividad de gestión en ambos switches.
- Acceso de consola a ambos switches.
- Todas las interfaces lógicas (LIF) del clúster de `up` estado sin necesidad de migrar.
- Personalización inicial del conmutador.
- Todos los puertos ISL habilitados y cableado.

Además, debe planificar, migrar y leer la documentación necesaria sobre conectividad de 10 GbE y 40/100 GbE desde los nodos a los switches de clúster Nexus 3132Q-V.

Migrar los switches

Acerca de los ejemplos

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

- Switches de clúster Nexus 3132Q-V, C1 y C2.
- Los nodos son n1 y n2.



Los ejemplos de este procedimiento utilizan dos nodos, cada uno utilizando dos puertos de interconexión de clúster de 40/100 GbE e4a y e4e. La ["Hardware Universe"](#) tiene detalles acerca de los puertos de clúster en las plataformas.

Acerca de esta tarea

Este procedimiento cubre los siguientes escenarios:

- n1_clus1 es la primera interfaz lógica del clúster (LIF) que se conecta al switch del clúster C1 para el nodo n1.
- n1_clus2 es la primera LIF del clúster que se conecta al switch de clúster C2 del nodo n1.

- n2_clus1 es la primera LIF de clúster que se conecta al switch de clúster C1 para el nodo n2.
- n2_clus2 es la segunda LIF del clúster que se conecta al switch de clúster C2 del nodo n2.
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del switch de red de clúster de Cisco ®" página](#).



Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 3000; los comandos de la ONTAP se usan a menos que se indique lo contrario.

- El clúster comienza con dos nodos conectados y funciona en una configuración de clúster sin switch de dos nodos.
- El primer puerto del clúster se mueve a C1.
- El segundo puerto del clúster se ha movido a C2.
- La opción de clúster sin switches de dos nodos está deshabilitada.

Paso 1: Preparación para la migración

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

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

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



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

2. Determine el estado administrativo u operativo de cada interfaz de clúster:

- a. Mostrar los atributos del puerto de red:

```
network port show
```

Muestra el ejemplo

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
-
e4e         Cluster      Cluster      up    9000 auto/40000 -
-

Node: n2

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
-
e4e         Cluster      Cluster      up    9000 auto/40000 -
-

4 entries were displayed.
```

b. Mostrar información acerca de las interfaces lógicas:

```
network interface show
```

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
e4a          n1_clus1    up/up      10.10.0.1/24      n1
true
e4e          n1_clus2    up/up      10.10.0.2/24      n1
true
e4a          n2_clus1    up/up      10.10.0.3/24      n2
true
e4e          n2_clus2    up/up      10.10.0.4/24      n2
true
4 entries were displayed.
```

3. Compruebe que los RCF e imagen adecuados están instalados en los nuevos conmutadores 3132Q-V según sea necesario para sus requisitos y realice las personalizaciones esenciales del sitio, como usuarios y contraseñas, direcciones de red, etc.

Debe preparar ambos switches en este momento. Si necesita actualizar el software RCF e Image, debe seguir estos pasos:

- a. Vaya a la ["Switches Ethernet de Cisco"](#) En el sitio de soporte de NetApp.
 - b. Anote el conmutador y las versiones de software necesarias en la tabla de esa página.
 - c. Descargue la versión adecuada de RCF.
 - d. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.
 - e. Descargue la versión adecuada del software Image.
4. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.

Paso 2: Mueva el primer puerto del clúster a C1

1. En los switches Nexus 3132Q-V C1 y C2, deshabilite todos los puertos orientados al nodo C1 y C2, pero no deshabilite los puertos ISL.

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos 1 a 30 desactivados en los switches del clúster de Nexus 3132Q-V C1 y C2 utilizando una configuración compatible con RCF

NX3132_RCF_v1.1_24p10g_26p40g.txt:

```
C1# copy running-config startup-config
[#####] 100%
Copy complete.
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# shutdown
C1(config-if-range)# exit
C1(config)# exit

C2# copy running-config startup-config
[#####] 100%
Copy complete.
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
```

2. Conecte los puertos 1/31 y 1/32 de C1 a los mismos puertos de C2 utilizando el cableado compatible.
3. Compruebe que los puertos ISL están operativos en C1 y C2:

```
show port-channel summary
```

Muestra el ejemplo

```
C1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      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)

C2# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      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)
```

4. Mostrar la lista de dispositivos vecinos en el conmutador:

```
show cdp neighbors
```


Muestra el ejemplo

```
C1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C2                  Eth1/31        174      R S I s          N3K-C3132Q-V
Eth1/31
C2                  Eth1/32        174      R S I s          N3K-C3132Q-V
Eth1/32

Total entries displayed: 2

C2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C1                  Eth1/31        178      R S I s          N3K-C3132Q-V
Eth1/31
C1                  Eth1/32        178      R S I s          N3K-C3132Q-V
Eth1/32

Total entries displayed: 2
```

5. Muestre la conectividad de puerto del clúster en cada nodo:

```
network device-discovery show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra una configuración de clúster sin switch de dos nodos.

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e4a	n2	e4a	FAS9000
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	n1	e4a	FAS9000
	e4e	n1	e4e	FAS9000

6. Migre la interfaz clus1 al puerto físico que aloja la clus2:

```
network interface migrate
```

Ejecute este comando desde cada nodo local.

Muestra el ejemplo

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1  
-source-node n1  
-destination-node n1 -destination-port e4e  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1  
-source-node n2  
-destination-node n2 -destination-port e4e
```

7. Compruebe la migración de las interfaces del clúster:

```
network interface show
```

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4e      false
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4e      false
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

8. Apague los puertos de clúster clus1 LIF en ambos nodos:

```
network port modify
```

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

9. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster
```

Muestra el ejemplo

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e4a 10.10.0.1
Cluster n1_clus2 n1      e4e 10.10.0.2
Cluster n2_clus1 n2      e4a 10.10.0.3
Cluster n2_clus2 n2      e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

10. Desconecte el cable del e4a del nodo n1.

Puede consultar la configuración en ejecución y conectar el primer puerto de 40 GbE en el conmutador C1 (puerto 1/7 en este ejemplo) a e4a en n1 usando el cableado compatible en Nexus 3132Q-V.



Al volver a conectar cualquier cable a un nuevo switch de clúster de Cisco, los cables utilizados deben ser de fibra o de cableado compatible con Cisco.

11. Desconecte el cable del e4a del nodo n2.

Puede consultar la configuración en ejecución y conectar e4a al siguiente puerto 40 GbE disponible en C1, puerto 1/8, utilizando el cableado compatible.

12. Habilite todos los puertos orientados al nodo en C1.

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos 1 a 30 activados en los switches de clúster C1 y C2 de Nexus 3132Q-V. mediante la configuración admitida en RCF

NX3132_RCF_v1.1_24p10g_26p40g.txt:

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

13. Active el primer puerto del clúster, e4a, en cada nodo:

```
network port modify
```

Muestra el ejemplo

```
cluster::*> network port modify -node n1 -port e4a -up-admin true
cluster::*> network port modify -node n2 -port e4a -up-admin true
```

14. Compruebe que los clústeres estén en ambos nodos:

```
network port show
```

Muestra el ejemplo

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

Node: n2

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

4 entries were displayed.
```

15. Para cada nodo, revierte todos los LIF de interconexión de clúster migrados:

```
network interface revert
```

Muestra el ejemplo

En el ejemplo siguiente se muestran los LIF migrados que se han revertido a sus puertos principales.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
```

16. Verifique que todos los puertos de interconexión de clúster ahora se reviertan a sus puertos raíz:

```
network interface show
```

La Is Home la columna debe mostrar un valor de true para todos los puertos enumerados en la Current Port columna. Si el valor mostrado es false, el puerto no se ha revertido.

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4a true n1_clus1 up/up 10.10.0.1/24 n1
e4e true n1_clus2 up/up 10.10.0.2/24 n1
e4a true n2_clus1 up/up 10.10.0.3/24 n2
e4e true n2_clus2 up/up 10.10.0.4/24 n2
4 entries were displayed.
```

Paso 3: Mueva el segundo puerto de clúster a C2

1. Muestre la conectividad de puerto del clúster en cada nodo:

```
network device-discovery show
```

Muestra el ejemplo

```
cluster::*> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	n1	e4e	FAS9000

2. En la consola de cada nodo, migre clus2 al puerto e4a:

```
network interface migrate
```

Muestra el ejemplo

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2  
-source-node n1  
-destination-node n1 -destination-port e4a  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2  
-source-node n2  
-destination-node n2 -destination-port e4a
```

3. Apague los puertos de clúster clus2 LIF en ambos nodos:

```
network port modify
```

En el ejemplo siguiente se muestran los puertos especificados que se están apagando en ambos nodos:

```
cluster::*> network port modify -node n1 -port e4e -up-admin false  
cluster::*> network port modify -node n2 -port e4e -up-admin false
```

4. Compruebe el estado de LIF del clúster:

```
network interface show
```


Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4a      false
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4a      false
4 entries were displayed.
```

5. Desconecte el cable del e4e en el nodo n1.

Puede consultar la configuración en ejecución y conectar el primer puerto de 40 GbE en el conmutador C2 (puerto 1/7 en este ejemplo) a e4e en la n1 usando el cableado compatible en la Nexus 3132Q-V.

6. Desconecte el cable del e4e en el nodo n2.

Puede consultar la configuración en ejecución y conectar e4e al siguiente puerto 40 GbE disponible en C2, puerto 1/8, utilizando el cableado compatible.

7. Habilite todos los puertos orientados al nodo en C2.

Muestra el ejemplo

En el ejemplo siguiente se muestran los puertos 1 a 30 activados en los switches de clúster C1 y C2 de Nexus 3132Q-V. mediante una configuración compatible con RCF

NX3132_RCF_v1.1_24p10g_26p40g.txt:

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

8. Active el segundo puerto del clúster, e4e, en cada nodo:

```
network port modify
```

En el siguiente ejemplo, se muestran los puertos especificados que se están subiendo:

```
cluster::*> network port modify -node n1 -port e4e -up-admin true
cluster::*> network port modify -node n2 -port e4e -up-admin true
```

9. Para cada nodo, revierte todos los LIF de interconexión de clúster migrados:

```
network interface revert
```

En el ejemplo siguiente se muestran los LIF migrados que se han revertido a sus puertos principales.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

10. Verifique que todos los puertos de interconexión de clúster ahora se reviertan a sus puertos raíz:

```
network interface show
```

La `Is Home` la columna debe mostrar un valor de `true` para todos los puertos enumerados en la `Current Port` columna. Si el valor mostrado es `false`, el puerto no se ha revertido.

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

11. Compruebe que todos los puertos de interconexión del clúster se encuentren en la `up` estado.

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

Muestra el ejemplo

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

Node: n2

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

4 entries were displayed.
```

Paso 4: Deshabilite la opción de clúster sin switch de dos nodos

1. Muestre los números de puertos del switch del clúster a los que está conectado cada puerto del clúster en cada nodo:

```
network device-discovery show
```

Muestra el ejemplo

```
cluster::*> network device-discovery show
```

Local		Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V

2. Mostrar switches de clúster detectados y supervisados:

```
system cluster-switch show
```

Muestra el ejemplo

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
C1 NX3132V	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.102
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

3. Deshabilite los ajustes de configuración de dos nodos sin switch en cualquier nodo:

```
network options switchless-cluster
```

```
network options switchless-cluster modify -enabled false
```

4. Compruebe que el switchless-cluster la opción se ha desactivado.

```
network options switchless-cluster show
```

Paso 5: Verificar la configuración

1. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster
```

Muestra el ejemplo

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e4a 10.10.0.1
Cluster n1_clus2 n1      e4e 10.10.0.2
Cluster n2_clus1 n2      e4a 10.10.0.3
Cluster n2_clus2 n2      e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

2. Habilite la función de recogida de registro de supervisión del estado del switch para recopilar archivos de registro relacionados con el switch:

```
system cluster-switch log setup-password
```

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

Muestra el ejemplo

```
cluster::*> **system cluster-switch log setup-password**
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

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

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

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

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

Enabling cluster switch log collection.

cluster::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

3. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:


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

Sustituya los interruptores

Requisitos para sustituir los switches de clúster Cisco Nexus 3132Q-V.

Asegúrese de comprender los requisitos de configuración, las conexiones de puertos y los requisitos de cableado al sustituir los switches de clúster.

Requisitos de Cisco Nexus 3132Q-V.

- Se admite el switch de clúster Cisco Nexus 3132Q-V.
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) página.
- Los switches de clúster utilizan los puertos de enlace entre switches (ISL) e1/31-32.
- La ["Hardware Universe"](#) Contiene información sobre el cableado compatible con los switches Nexus 3132Q-V:
 - Los nodos con conexiones de clúster de 10 GbE requieren módulos ópticos QSFP con cables de fibra de cable multiconector o cables de cobre QSFP a SFP+.
 - Los nodos con conexiones de clúster de 40/100 GbE requieren módulos ópticos QSFP/QSFP28 compatibles con cables de fibra o cables de conexión directa de cobre QSFP/QSFP28.
 - Los switches de clúster utilizan el cableado ISL adecuado: 2 cables de conexión directa de cobre o fibra QSFP28.
- En Nexus 3132Q-V, puede utilizar puertos QSFP como Ethernet de 40/100 GB o modos Ethernet de 4 x10 GB.

De forma predeterminada, hay 32 puertos en el modo Ethernet de 40/100 GB. Estos puertos Ethernet de 40 GB están numerados en una convención de nomenclatura de 2 tubos. Por ejemplo, el segundo puerto Ethernet de 40 GB está numerado como 1/2. El proceso de cambiar la configuración de Ethernet de 40 GB a Ethernet de 10 GB se denomina *breakout* y el proceso de cambiar la configuración de Ethernet de 10 GB a Ethernet de 40 GB se denomina *breakin*. Cuando se rompe un puerto Ethernet de 40/100 GB en puertos Ethernet de 10 GB, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tubos. Por ejemplo, los puertos de arranque del segundo puerto Ethernet de 40/100 GB están numerados como 1/2/1, 1/2/2, 1/2/3, 1/2/4.

- En el lado izquierdo de Nexus 3132Q-V se encuentra un conjunto de cuatro puertos SFP+ multiplexados al primer puerto QSFP.

De forma predeterminada, el RCF está estructurado para utilizar el primer puerto QSFP.

Puede hacer que cuatro puertos SFP+ estén activos en lugar de un puerto QSFP para Nexus 3132Q-V mediante el `hardware profile front portmode sfp-plus` comando. Del mismo modo, se puede restablecer Nexus 3132Q-V para utilizar un puerto QSFP en lugar de cuatro puertos SFP+ mediante el `hardware profile front portmode qsfp` comando.

- Debe haber configurado algunos de los puertos en Nexus 3132Q-V para que funcionen a 10 GbE o 40/100 GbE.

Puede extraer los primeros seis puertos en modo 4x10 GbE mediante el `interface breakout module`

1 port 1-6 map 10g-4x comando. De forma similar, puede volver a agrupar los primeros seis puertos QSFP+ de la configuración de cable mediante el no interface breakout module 1 port 1-6 map 10g-4x comando.

- Debe haber realizado la planificación, la migración y leer la documentación necesaria en conectividad de 10 GbE y 40/100 GbE desde los nodos a los switches de clúster Nexus 3132Q-V.

La "[Switches Ethernet de Cisco](#)" La página tiene información acerca de las versiones ONTAP y NX-OS que se admiten en este procedimiento.

Requisitos de Cisco Nexus 5596

- Se admiten los siguientes switches de clúster:
 - Nexus 5596
 - Nexus 3132Q-V
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la "[Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®](#)" página.
- Los switches de clúster utilizan los siguientes puertos para las conexiones a los nodos:
 - Puertos e1/1-40 (10 GbE): Nexus 5596
 - Puertos e1/1-30 (40/100 GbE): Nexus 3132Q-V
- Los switches de clúster utilizan los siguientes puertos de enlace entre switches (ISL):
 - Puertos e1/41-48 (10 GbE): Nexus 5596
 - Puertos e1/31-32 (40/100 GbE): Nexus 3132Q-V
- La "[Hardware Universe](#)" Contiene información sobre el cableado compatible con los switches Nexus 3132Q-V:
 - Los nodos con conexiones de clúster de 10 GbE requieren cables de fibra óptica QSFP a SFP+ o cables de cobre QSFP a SFP+.
 - Los nodos con conexiones de clúster de 40/100 GbE requieren módulos ópticos QSFP/QSFP28 admitidos con cables de fibra o cables de conexión directa de cobre QSFP/QSFP28.
- Los switches de clúster utilizan el cableado ISL adecuado:
 - Principio: De Nexus 5596 a Nexus 5596 (de SFP+ a SFP+)
 - 8 cables de conexión directa de cobre o fibra SFP+
 - Provisional: Nexus 5596 a Nexus 3132Q-V (QSFP a 4 partes SFP+)
 - 1 cables QSFP a SFP+ de fibra óptica o cables de interrupción de cobre
 - Final: Nexus 3132Q-V a Nexus 3132Q-V (QSFP28 a QSFP28)
 - 2 cables de conexión directa de cobre o fibra QSFP28
- En los switches Nexus 3132Q-V, puede utilizar puertos QSFP/QSFP28 como 40/100 modos Ethernet Gigabit o 4 modos Ethernet Gigabit 10.

De forma predeterminada, hay 32 puertos en el modo 40/100 Gigabit Ethernet. Estos puertos 40 Gigabit Ethernet están numerados en una convención de nomenclatura de 2 tubos. Por ejemplo, el segundo puerto 40 Gigabit Ethernet está numerado como 1/2. El proceso de cambiar la configuración de 40 Gigabit Ethernet a 10 Gigabit Ethernet se denomina *breakout* y el proceso de cambiar la configuración de 10 Gigabit Ethernet a 40 Gigabit Ethernet se denomina *breakin*. Cuando se dividen un puerto 40/100 Gigabit

Ethernet en 10 puertos Gigabit Ethernet, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tupla. Por ejemplo, los puertos de salida del segundo puerto Ethernet 40 Gigabit están numerados como 1/2/1, 1/2/2, 1/2/3 y 1/2/4.

- En el lado izquierdo de los conmutadores Nexus 3132Q-V hay un conjunto de 4 puertos SFP+ multiplexados a ese puerto QSFP28.

De forma predeterminada, el RCF está estructurado para utilizar el puerto QSFP28.



Puede activar 4 puertos SFP+ en lugar de un puerto QSFP para los switches Nexus 3132Q-V mediante el `hardware profile front portmode sfp-plus` comando. De forma similar, puede restablecer los switches Nexus 3132Q-V para utilizar un puerto QSFP en lugar de 4 puertos SFP+ mediante el `hardware profile front portmode qsfp` comando.

- Ha configurado algunos de los puertos en los switches Nexus 3132Q-V para que funcionen a 10 GbE o 40/100 GbE.



Puede dividir los primeros seis puertos en modo 4x10 GbE mediante el `interface breakout module 1 port 1-6 map 10g-4x` comando. De forma similar, puede volver a agrupar los primeros seis puertos QSFP+ de la configuración de cable mediante el `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Ha realizado la planificación, la migración y lea la documentación necesaria sobre conectividad 10 GbE y 40/100 GbE desde los nodos a los switches de clúster Nexus 3132Q-V.
- Las versiones ONTAP y NX-OS compatibles con este procedimiento son en la ["Switches Ethernet de Cisco"](#) página.

Requisitos de CN1610 de NetApp

- Se admiten los siguientes switches de clúster:
 - CN1610 de NetApp
 - Cisco Nexus 3132Q-V
- Los switches de clúster admiten las siguientes conexiones de nodo:
 - NetApp CN1610: Puertos 0/1 a 0/12 (10 GbE)
 - Cisco Nexus 3132Q-V: Puertos e1/1-30 (40/100 GbE)
- Los switches de clúster utilizan los siguientes puertos de enlace entre switches (ISL):
 - NetApp CN1610: Puertos 0/13 a 0/16 (10 GbE)
 - Cisco Nexus 3132Q-V: Puertos e1/31-32 (40/100 GbE)
- La ["Hardware Universe"](#) Contiene información sobre el cableado compatible con los switches Nexus 3132Q-V:
 - Los nodos con conexiones de clúster de 10 GbE requieren cables de fibra óptica QSFP a SFP+ o cables de cobre QSFP a SFP+
 - Los nodos con conexiones de clúster de 40/100 GbE requieren módulos ópticos QSFP/QSFP28 admitidos con cables de fibra óptica o cables de conexión directa de cobre QSFP/QSFP28
- El cableado ISL adecuado es el siguiente:
 - Comenzando: Para CN1610 a CN1610 (SFP+ a SFP+), cuatro cables de conexión directa o fibra

óptica SFP+

- Provisional: Para CN1610 a Nexus 3132Q-V (QSFP a cuatro SFP+), un cable de fibra óptica o cobre QSFP a SFP+
 - Final: Para Nexus 3132Q-V a Nexus 3132Q-V (QSFP28 a QSFP28), dos cables de conexión directa de cobre o fibra óptica QSFP28
- Los cables twinax de NetApp no son compatibles con los switches Cisco Nexus 3132Q-V.

Si su configuración actual del CN1610 utiliza cables twinax de NetApp para conexiones clúster-nodo-switch o conexiones ISL y quiere seguir utilizando twinax en su entorno, debe procurar los cables twinax de Cisco. Como alternativa, puede utilizar cables de fibra óptica para las conexiones ISL y las conexiones cluster-nodo-switch.

- En los switches Nexus 3132Q-V, puede utilizar puertos QSFP/QSFP28 como modos Ethernet de 40/100 GB o Ethernet 4x 10 GB.

De forma predeterminada, hay 32 puertos en el modo Ethernet de 40/100 GB. Estos puertos Ethernet de 40 GB están numerados en una convención de nomenclatura de 2 tubos. Por ejemplo, el segundo puerto Ethernet de 40 GB está numerado como 1/2. El proceso de cambiar la configuración de Ethernet de 40 GB a Ethernet de 10 GB se denomina *breakout* y el proceso de cambiar la configuración de Ethernet de 10 GB a Ethernet de 40 GB se denomina *breakin*. Cuando se rompe un puerto Ethernet de 40/100 GB en puertos Ethernet de 10 GB, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tubos. Por ejemplo, los puertos de arranque del segundo puerto Ethernet de 40 GB están numerados como 1/2/1, 1/2/2, 1/2/3 y 1/2/4.

- En el lado izquierdo de los conmutadores Nexus 3132Q-V hay un conjunto de cuatro puertos SFP+ multiplexados al primer puerto QSFP.

De forma predeterminada, el archivo de configuración de referencia (RCF) está estructurado para utilizar el primer puerto QSFP.

Puede hacer que cuatro puertos SFP+ estén activos en lugar de un puerto QSFP para los switches Nexus 3132Q-V mediante el `hardware profile front portmode sfp-plus` comando. De forma similar, puede restablecer los switches Nexus 3132Q-V para utilizar un puerto QSFP en lugar de cuatro puertos SFP+ mediante el `hardware profile front portmode qsfp` comando.



Cuando se utilizan los primeros cuatro puertos SFP+, éste deshabilitará el primer puerto QSFP de 40 GbE.

- Debe haber configurado algunos de los puertos en los switches Nexus 3132Q-V para que funcionen a 10 GbE o 40/100 GbE.

Puede dividir los primeros seis puertos en 4 puertos 10 GbE en modo mediante el `interface breakout module 1 port 1-6 map 10g-4x` comando. De forma similar, puede volver a agrupar los primeros seis puertos QSFP+ de la configuración *breakout* mediante el `no interface breakout module 1 port 1-6 map 10g-4x` comando.

- Debe haber realizado la planificación, la migración y leer la documentación necesaria en conectividad de 10 GbE y 40/100 GbE desde los nodos a los switches de clúster Nexus 3132Q-V.
- Las versiones ONTAP y NX-OS compatibles con este procedimiento se enumeran en la ["Switches Ethernet de Cisco"](#) página.
- Las versiones ONTAP Y FASTPATH compatibles con este procedimiento se enumeran en la ["Switches CN1601 y CN1610 de NetApp"](#) página.

Sustituya los switches de clúster Cisco Nexus 3132Q-V.

Siga este procedimiento para sustituir un switch Cisco Nexus 3132Q-V defectuoso en una red de clúster. El procedimiento de sustitución es un procedimiento no disruptivo (NDO).

Revise los requisitos

Requisitos de switch

Revise la ["Requisitos para sustituir los switches de clúster Cisco Nexus 3132Q-V."](#)

Lo que necesitará

- La configuración de clúster y red existente tiene:
 - La infraestructura de clúster Nexus 3132Q-V es redundante y completamente funcional en ambos switches.

La ["Switch Ethernet de Cisco"](#) Page tiene las últimas versiones RCF y NX-OS en sus switches.

 - Todos los puertos del clúster están en la `up` estado.
 - La conectividad de gestión existe en ambos switches.
 - Todas las interfaces lógicas (LIF) del clúster están en la `up` estado y se han migrado.
- Para el interruptor de sustitución Nexus 3132Q-V, asegúrese de que:
 - La conectividad de la red de gestión en el switch de reemplazo es funcional.
 - El acceso de la consola al interruptor de sustitución está en su lugar.
 - El conmutador de imagen del sistema operativo RCF y NX-OS deseado se carga en el conmutador.
 - Se ha completado la personalización inicial del conmutador.
- ["Hardware Universe"](#)

Sustituya el interruptor

Este procedimiento sustituye al segundo interruptor de grupo de Nexus 3132Q-V CL2 con el nuevo interruptor C2 3132Q-V.

Acerca de los ejemplos

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

- `n1_clus1` es la primera interfaz lógica del clúster (LIF) conectada al switch del clúster C1 para el nodo n1.
- `n1_clus2` es la primera LIF del clúster conectada al switch de clúster CL2 o C2 para el nodo n1.
- `n1_clus3` es la segunda LIF conectada al switch de clúster C2 para el nodo n1.
- `n1_clus4` es la segunda LIF conectada al switch de clúster CL1, para el nodo n1.
- El número de puertos 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en la ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) página.
- Los nodos son n1, n2, n3 y n4. - Los ejemplos de este procedimiento emplean cuatro nodos: Dos nodos utilizan cuatro puertos de interconexión de clúster de 10 GB: E0a, e0b, e0c y e0d. Los otros dos nodos utilizan dos puertos de interconexión de clúster de 40 GB: e4a y e4e. Consulte ["Hardware Universe"](#) para los puertos del clúster reales en las plataformas.

Acerca de esta tarea

Este procedimiento cubre el siguiente caso:

- El clúster comienza con cuatro nodos conectados a dos switches de cluster Nexus 3132Q-V, CL1 y CL2.
- El switch del clúster CL2 debe ser sustituido por C2
 - En cada nodo, las LIF de clúster conectadas a CL2 se migran a los puertos del clúster conectados a CL1.
 - Desconecte el cableado de todos los puertos del CL2 y vuelva a conectar el cableado a los mismos puertos del conmutador C2 de sustitución.
 - En cada nodo, sus LIF de clúster migrados se revierten.

Paso 1: Prepararse para la sustitución

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

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

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



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

2. Muestra información sobre los dispositivos de la configuración:

```
network device-discovery show
```

Muestra el ejemplo

```
cluster::> network device-discovery show
```

Local		Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e0a	CL1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	CL2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	CL2	Ethernet1/1/2	N3K-C3132Q-V
n2	e0d	CL1	Ethernet1/1/2	N3K-C3132Q-V
	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	CL2	Ethernet1/1/3	N3K-C3132Q-V
n3	e0c	CL2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	CL1	Ethernet1/1/4	N3K-C3132Q-V
	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3132Q-V
n4	e4e	CL2	Ethernet1/7	N3K-C3132Q-V
	/cdp			
	e4a	CL1	Ethernet1/8	N3K-C3132Q-V
	e4e	CL2	Ethernet1/8	N3K-C3132Q-V

```
12 entries were displayed
```

3. Determine el estado administrativo u operativo de cada interfaz de clúster:

a. Mostrar los atributos del puerto de red:

```
network port show
```

Muestra el ejemplo

```
cluster::*> network port show -role cluster
(network port show)
```

Node: n1

Ignore

		Speed (Mbps)				
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/10000 -
-						
e0b	Cluster	Cluster		up	9000	auto/10000 -
-						
e0c	Cluster	Cluster		up	9000	auto/10000 -
-						
e0d	Cluster	Cluster		up	9000	auto/10000 -
-						

Node: n2

Ignore

		Speed (Mbps)				
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/10000 -
-						
e0b	Cluster	Cluster		up	9000	auto/10000 -
-						
e0c	Cluster	Cluster		up	9000	auto/10000 -
-						
e0d	Cluster	Cluster		up	9000	auto/10000 -
-						

Node: n3

Ignore

		Speed (Mbps)				
Health	Health					


```

Port      IPspace    Broadcast Domain Link MTU  Admin/Oper
Status    Status
-----
-----
e4a      Cluster   Cluster           up   9000 auto/40000 -
-
e4e      Cluster   Cluster           up   9000 auto/40000 -
-

Node: n4

Ignore

Speed (Mbps)
Health    Health
Port      IPspace    Broadcast Domain Link MTU  Admin/Oper
Status    Status
-----
-----
e4a      Cluster   Cluster           up   9000 auto/40000 -
-
e4e      Cluster   Cluster           up   9000 auto/40000 -
-

12 entries were displayed.

```

b. Mostrar información acerca de las interfaces lógicas:

```
network interface show
```

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
```

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

Cluster					
e0a	true	n1_clus1	up/up	10.10.0.1/24	n1
e0b	true	n1_clus2	up/up	10.10.0.2/24	n1
e0c	true	n1_clus3	up/up	10.10.0.3/24	n1
e0d	true	n1_clus4	up/up	10.10.0.4/24	n1
e0a	true	n2_clus1	up/up	10.10.0.5/24	n2
e0b	true	n2_clus2	up/up	10.10.0.6/24	n2
e0c	true	n2_clus3	up/up	10.10.0.7/24	n2
e0d	true	n2_clus4	up/up	10.10.0.8/24	n2
e0a	true	n3_clus1	up/up	10.10.0.9/24	n3
e0e	true	n3_clus2	up/up	10.10.0.10/24	n3
e0a	true	n4_clus1	up/up	10.10.0.11/24	n4
e0e	true	n4_clus2	up/up	10.10.0.12/24	n4

12 entries were displayed.

c. Muestre la información sobre los switches del clúster detectados:

```
system cluster-switch show
```

Muestra el ejemplo

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
CL2 NX3132V	cluster-network	10.10.1.102
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

4. Compruebe que el RCF y la imagen adecuados están instalados en el nuevo switch Nexus 3132Q-V, según sea necesario, y realice las personalizaciones esenciales del sitio.

Debe preparar el interruptor de sustitución en este momento. Si necesita actualizar el RCF y la imagen, debe seguir estos pasos:

- a. En el sitio de soporte de NetApp, vaya a ["Switch Ethernet de Cisco"](#) página.
 - b. Anote el conmutador y las versiones de software necesarias en la tabla de esa página.
 - c. Descargue la versión adecuada del RCF.
 - d. Haga clic en **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.
 - e. Descargue la versión adecuada del software Image.
5. Migre las LIF asociadas a los puertos del clúster conectados al switch C2:

```
network interface migrate
```

Muestra el ejemplo

Este ejemplo muestra que la migración LIF se realiza en todos los nodos:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -destination-node n2 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2
-source-node n3 -destination-node n3 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2
-source-node n4 -destination-node n4 -destination-port e4a
```

6. Compruebe el estado del clúster:

```
network interface show
```

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
(network interface show)
```

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

Cluster				
e0a	n1_clus1	up/up	10.10.0.1/24	n1
e0a	n1_clus2	up/up	10.10.0.2/24	n1
e0d	n1_clus3	up/up	10.10.0.3/24	n1
e0d	n1_clus4	up/up	10.10.0.4/24	n1
e0a	n2_clus1	up/up	10.10.0.5/24	n2
e0a	n2_clus2	up/up	10.10.0.6/24	n2
e0d	n2_clus3	up/up	10.10.0.7/24	n2
e0d	n2_clus4	up/up	10.10.0.8/24	n2
e4a	n3_clus1	up/up	10.10.0.9/24	n3
e4a	n3_clus2	up/up	10.10.0.10/24	n3
e4a	n4_clus1	up/up	10.10.0.11/24	n4
e4a	n4_clus2	up/up	10.10.0.12/24	n4

12 entries were displayed.

7. Apague los puertos de interconexión de clúster que estén conectados físicamente al switch CL2:

```
network port modify
```

Muestra el ejemplo

En este ejemplo, se muestran los puertos especificados que se están apagando en todos los nodos:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster
```

Muestra el ejemplo

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8
Cluster n3_clus1 n4      e0a 10.10.0.9
Cluster n3_clus2 n3      e0e 10.10.0.10
Cluster n4_clus1 n4      e0a 10.10.0.11
Cluster n4_clus2 n4      e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.1 to Remote 10.10.0.9
  Local 10.10.0.1 to Remote 10.10.0.10
  Local 10.10.0.1 to Remote 10.10.0.11
  Local 10.10.0.1 to Remote 10.10.0.12
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.9
  Local 10.10.0.2 to Remote 10.10.0.10
  Local 10.10.0.2 to Remote 10.10.0.11
  Local 10.10.0.2 to Remote 10.10.0.12
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
```

```
Local 10.10.0.3 to Remote 10.10.0.7
Local 10.10.0.3 to Remote 10.10.0.8
Local 10.10.0.3 to Remote 10.10.0.9
Local 10.10.0.3 to Remote 10.10.0.10
Local 10.10.0.3 to Remote 10.10.0.11
Local 10.10.0.3 to Remote 10.10.0.12
Local 10.10.0.4 to Remote 10.10.0.5
Local 10.10.0.4 to Remote 10.10.0.6
Local 10.10.0.4 to Remote 10.10.0.7
Local 10.10.0.4 to Remote 10.10.0.8
Local 10.10.0.4 to Remote 10.10.0.9
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
```

Larger than PMTU communication succeeds on 32 path(s)

RPC status:

8 paths up, 0 paths down (tcp check)

8 paths up, 0 paths down (udp check)

9. Apague los puertos 1/31 y 1/32 de CL1 y el interruptor Nexus 3132Q-V activo:

shutdown

Muestra el ejemplo

En este ejemplo, se muestran los puertos ISL 1/31 y 1/32 que se están apagando en el switch CL1:

```
(CL1)# configure
(CL1) (Config)# interface e1/31-32
(CL1(config-if-range)# shutdown
(CL1(config-if-range)# exit
(CL1) (Config)# exit
(CL1)#
```

Paso 2: Configurar puertos

1. Retire todos los cables conectados al conmutador Nexus 3132Q-V CL2 y vuelva a conectarlos al conmutador C2 de sustitución en todos los nodos.
2. Quite los cables ISL de los puertos e1/31 y e1/32 en CL2 y vuelva a conectarlos a los mismos puertos en el switch de reemplazo C2.
3. Traiga los puertos ISL 1/31 y 1/32 en el switch Nexus 3132Q-V CL1:


```
(CL1)# configure
(CL1) (Config)# interface e1/31-32
(CL1(config-if-range)# no shutdown
(CL1(config-if-range)# exit
(CL1) (Config)# exit
(CL1)#
```

4. Verifique que los ISL estén activos en CL1:

```
show port-channel
```

Los puertos eth1/31 y eth1/32 deben indicar (P) , Lo que significa que los puertos ISL están activos en el canal de puerto.

Muestra el ejemplo

```
CL1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      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)
```

5. Compruebe que los ISL estén activos en C2:

```
show port-channel summary
```

Los puertos eth1/31 y eth1/32 deben indicar (P) , Lo que significa que ambos puertos ISL están en el canal de puerto.

Muestra el ejemplo

```
C2# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      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)
```

6. En todos los nodos, active todos los puertos de interconexión del clúster conectados al switch C2 de Nexus 3132Q-V:

```
network port modify
```

Muestra el ejemplo

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
cluster::*> network port modify -node n3 -port e4e -up-admin true
cluster::*> network port modify -node n4 -port e4e -up-admin true
```

7. Para todos los nodos, revierte todos los LIF de interconexión del clúster migrados:

```
network interface revert
```

Muestra el ejemplo

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
Cluster::*> network interface revert -vserver Cluster -lif n3_clus2
Cluster::*> network interface revert -vserver Cluster -lif n4_clus2
```

8. Compruebe que los puertos de interconexión de clúster ahora se han revertido a su origen:

```
network interface show
```

Muestra el ejemplo

Este ejemplo muestra que todas las LIF se han revertido correctamente porque los puertos enumerados en Current Port la columna tiene el estado de true en la Is Home columna. Si la Is Home el valor de columna es false, El LIF no se ha revertido.

```
cluster::*> network interface show -role cluster
(network interface show)
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

12 entries were displayed.

9. Compruebe que los puertos del clúster están conectados:

```
network port show
```

Muestra el ejemplo

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

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

```
Node: n2
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

```
Node: n3
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status

```

Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000 -
-
e4e      Cluster      Cluster      up    9000 auto/40000 -
-

Node: n4

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000 -
-
e4e      Cluster      Cluster      up    9000 auto/40000 -
-

12 entries were displayed.

```

10. Hacer ping a las interfaces remotas del clúster y realizar una comprobación del servidor RPC:

```
cluster ping-cluster
```

Muestra el ejemplo

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8
Cluster n3_clus1 n3      e0a 10.10.0.9
Cluster n3_clus2 n3      e0e 10.10.0.10
Cluster n4_clus1 n4      e0a 10.10.0.11
Cluster n4_clus2 n4      e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
```

```
Local 10.10.0.3 to Remote 10.10.0.7
Local 10.10.0.3 to Remote 10.10.0.8
Local 10.10.0.3 to Remote 10.10.0.9
Local 10.10.0.3 to Remote 10.10.0.10
Local 10.10.0.3 to Remote 10.10.0.11
Local 10.10.0.3 to Remote 10.10.0.12
Local 10.10.0.4 to Remote 10.10.0.5
Local 10.10.0.4 to Remote 10.10.0.6
Local 10.10.0.4 to Remote 10.10.0.7
Local 10.10.0.4 to Remote 10.10.0.8
Local 10.10.0.4 to Remote 10.10.0.9
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
```

Larger than PMTU communication succeeds on 32 path(s)

RPC status:

8 paths up, 0 paths down (tcp check)

8 paths up, 0 paths down (udp check)

Paso 3: Verificar la configuración

1. Muestra la información sobre los dispositivos de la configuración:

- ° network device-discovery show
- ° network port show -role cluster
- ° network interface show -role cluster
- ° system cluster-switch show

Muestra el ejemplo

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/2	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/3	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/4	N3K-C3132Q-V
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V

12 entries were displayed.

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

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Speed(Mbps)	Health Status
	e0a	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0b	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0c	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0d	Cluster	Cluster	up	9000	auto/10000	-	
	-							

Node: n2

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

Node: n3

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							
e4e	Cluster	Cluster		up	9000	auto/40000	-
-							

Node: n4

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							
e4e	Cluster	Cluster		up	9000	auto/40000	-
-							

12 entries were displayed.

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

```
(network interface show)
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

12 entries were displayed.

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
CL2 NX3132V	cluster-network	10.10.1.102
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000003		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

3 entries were displayed.

2. Retire el interruptor Nexus 3132Q-V sustituido si no se ha retirado automáticamente:

```
system cluster-switch delete
```

```
cluster::*> system cluster-switch delete -device CL2
```

3. Compruebe que se supervisan los switches de clúster adecuados:

```
system cluster-switch show
```

Muestra el ejemplo

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

4. Habilite la función de recogida de registro de supervisión del estado del switch para recopilar archivos de registro relacionados con el switch:

```
system cluster-switch log setup-password
```

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

Muestra el ejemplo

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

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

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

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

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

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

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

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

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

Enabling cluster switch log collection.

cluster::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

5. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

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

Sustituya los switches de clúster Cisco Nexus 3132Q-V por conexiones sin switches

Puede migrar desde un clúster con una red de clúster conmutada a uno donde dos nodos están conectados directamente para ONTAP 9.3 y versiones posteriores.

Revise los requisitos

Directrices

Revise las siguientes directrices:

- La migración a una configuración de clúster de dos nodos sin switch es una operación no disruptiva. La mayoría de los sistemas tienen dos puertos de interconexión de clúster dedicados en cada nodo, pero también puede usar este procedimiento para sistemas con un número mayor de puertos de interconexión de clúster dedicados en cada nodo, como cuatro, seis u ocho.
- No se puede usar la función de interconexión de clúster sin switches con más de dos nodos.
- Si tiene un clúster de dos nodos existente que utiliza switches de interconexión de clúster y ejecuta ONTAP 9.3 o una versión posterior, puede reemplazar los switches por conexiones directas de vuelta a atrás entre los nodos.

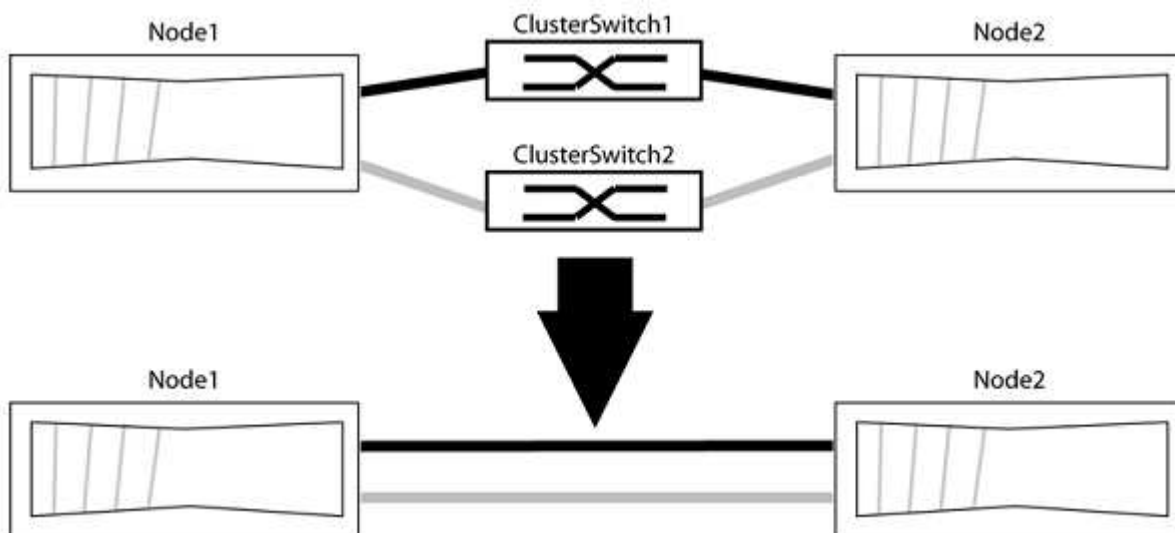
Lo que necesitará

- Un clúster en buen estado que consta de dos nodos conectados por switches de clúster. Los nodos deben ejecutar la misma versión de ONTAP.
- Cada nodo con el número requerido de puertos de clúster dedicados, que proporcionan conexiones redundantes de interconexión de clúster para admitir la configuración de su sistema. Por ejemplo, hay dos puertos redundantes para un sistema con dos puertos de Cluster Interconnect dedicados en cada nodo.

Migrar los switches

Acercas de esta tarea

En el siguiente procedimiento, se quitan los switches de clúster de dos nodos y se reemplaza cada conexión al switch por una conexión directa al nodo compañero.



Acerca de los ejemplos

Los ejemplos del siguiente procedimiento muestran nodos que utilizan «e0a» y «e0b» como puertos del clúster. Sus nodos pueden usar distintos puertos de clúster según varían según el sistema.

Paso 1: Preparación para la migración

1. Cambie el nivel de privilegio a Advanced, introduzca `y` cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado `*>` aparece.

2. ONTAP 9.3 y versiones posteriores admiten la detección automática de clústeres sin switch, que está habilitado de forma predeterminada.

Puede verificar que la detección de clústeres sin switch esté habilitada mediante el comando de privilegio avanzado:

```
network options detect-switchless-cluster show
```

Muestra el ejemplo

El siguiente resultado de ejemplo muestra si la opción está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Si la opción "Activar detección de clústeres sin switch" es `false` Póngase en contacto con el soporte de NetApp.

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

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

donde `h` es la duración del plazo de mantenimiento en horas. El mensaje notifica al soporte técnico de esta tarea de mantenimiento para que estos puedan impedir la creación automática de casos durante la ventana de mantenimiento.

En el ejemplo siguiente, el comando suprime la creación automática de casos durante dos horas:

Muestra el ejemplo

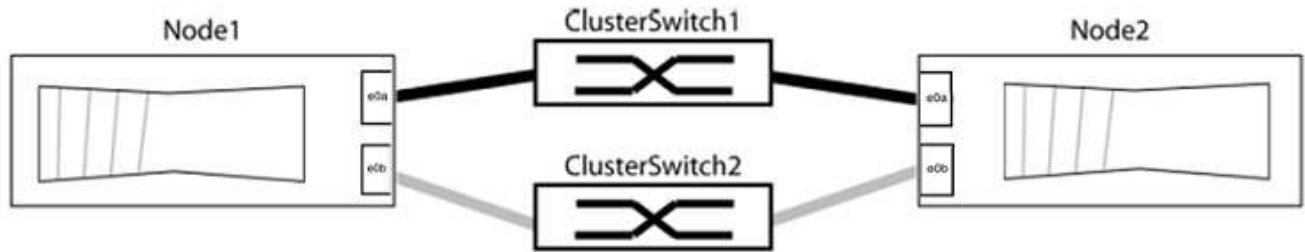
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```


Paso 2: Configure los puertos y el cableado

1. Organice los puertos del clúster en cada switch en grupos de modo que los puertos del clúster en group1 vayan a Cluster switch1 y los puertos del cluster en group2 vayan a cluster switch2. Estos grupos son necesarios más adelante en el procedimiento.
2. Identificar los puertos del clúster y verificar el estado y el estado del enlace:

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

En el siguiente ejemplo, en el caso de nodos con puertos de clúster "e0a" y "e0b", un grupo se identifica como "1:e0a" y "2:e0a" y el otro grupo como "1:e0b" y "2:e0b". Sus nodos pueden usar puertos de clúster diferentes porque varían según el sistema.



Compruebe que los puertos tienen un valor de `up` Para la columna "Link" y un valor de `healthy` Para la columna "Estado de salud".

Muestra el ejemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

3. Confirmar que todas las LIF de clúster están en sus puertos raíz.

Compruebe que la columna "es-home" es true Para cada LIF del clúster:

```
network interface show -vserver Cluster -fields is-home
```

Muestra el ejemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif           is-home
-----  -
Cluster  node1_clus1   true
Cluster  node1_clus2   true
Cluster  node2_clus1   true
Cluster  node2_clus2   true
4 entries were displayed.
```

Si hay LIF de clúster que no estén en sus puertos raíz, revierte estos LIF a sus puertos principales:

```
network interface revert -vserver Cluster -lif *
```

4. Deshabilite la reversión automática para las LIF del clúster:

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

5. Compruebe que todos los puertos enumerados en el paso anterior están conectados a un conmutador de red:

```
network device-discovery show -port cluster_port
```

La columna “dispositivo detectado” debe ser el nombre del conmutador de clúster al que está conectado el puerto.

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster «e0a» y «e0b» están conectados correctamente a los switches del clúster «cs1» y «cs2».

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e0a    cs1                      0/11       BES-53248
          e0b    cs2                      0/12       BES-53248
node2/cdp
          e0a    cs1                      0/9        BES-53248
          e0b    cs2                      0/9        BES-53248
4 entries were displayed.
```

6. Compruebe la conectividad del clúster:

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

7. Compruebe que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

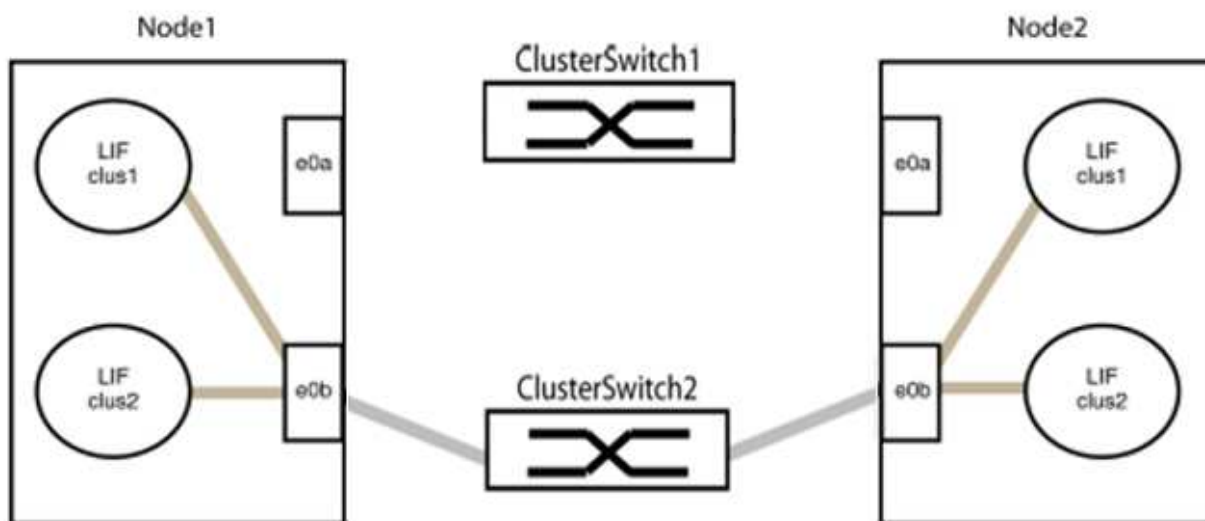
8. Configure la configuración sin switches para los puertos del grupo 1.



Para evitar posibles problemas de red, debe desconectar los puertos del grupo 1 y volver a conectarlos lo antes posible, por ejemplo, **en menos de 20 segundos**.

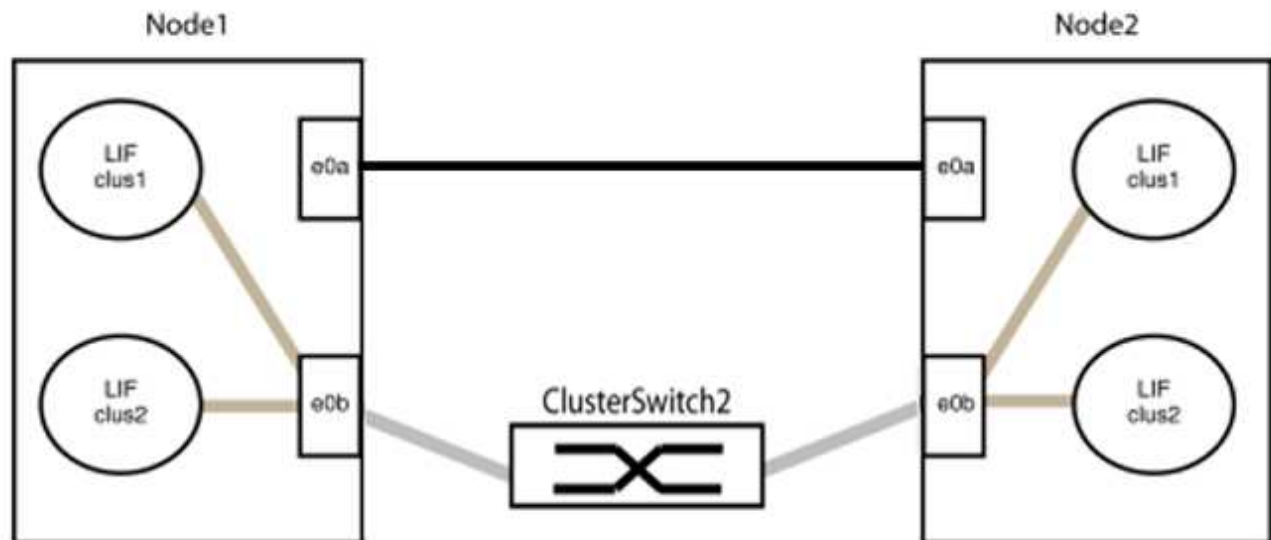
a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

En el ejemplo siguiente, los cables se desconectan del puerto "e0a" en cada nodo, y el tráfico del clúster continúa a través del switch y el puerto "e0b" en cada nodo:



b. Conecte los puertos en group1 de vuelta a espalda.

En el siguiente ejemplo, "e0a" en el nodo 1 está conectado a "e0a" en el nodo 2:



9. La opción de red de clúster sin switch desde la transición `false` para `true`. Esto puede tardar hasta 45 segundos. Confirme que la opción sin switches está establecida en `true`:

```
network options switchless-cluster show
```

En el siguiente ejemplo se muestra que el clúster sin switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

10. Compruebe que la red de clúster no se haya interrumpido:

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



Antes de continuar con el siguiente paso, debe esperar al menos dos minutos para confirmar una conexión de retroceso en funcionamiento en el grupo 1.

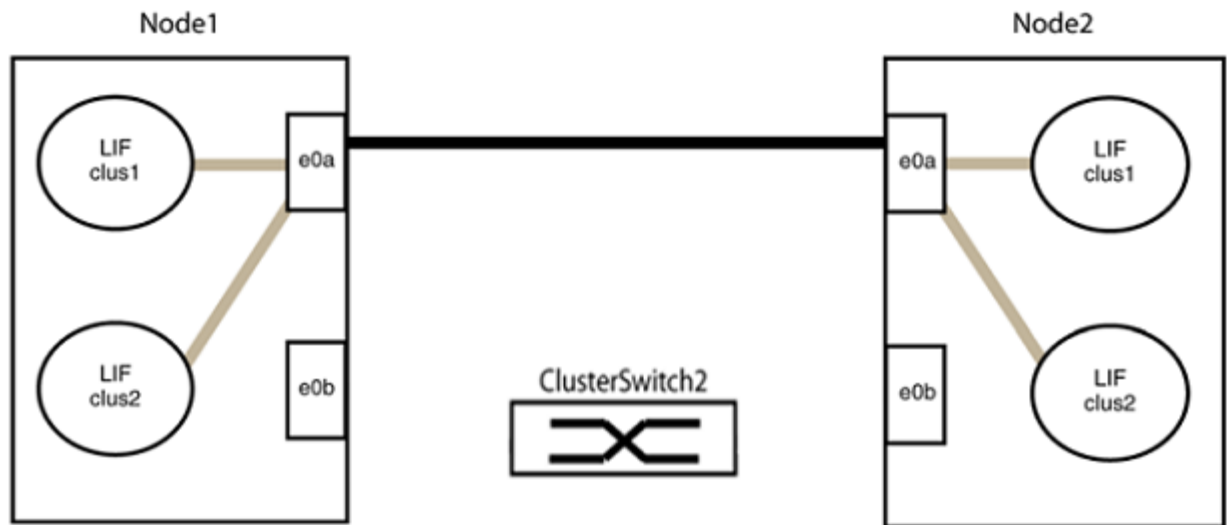
11. Configure la configuración sin switches para los puertos del grupo 2.



Para evitar posibles problemas de red, debe desconectar los puertos del grupo 2 y volver a conectarlos lo antes posible, por ejemplo, **en menos de 20 segundos**.

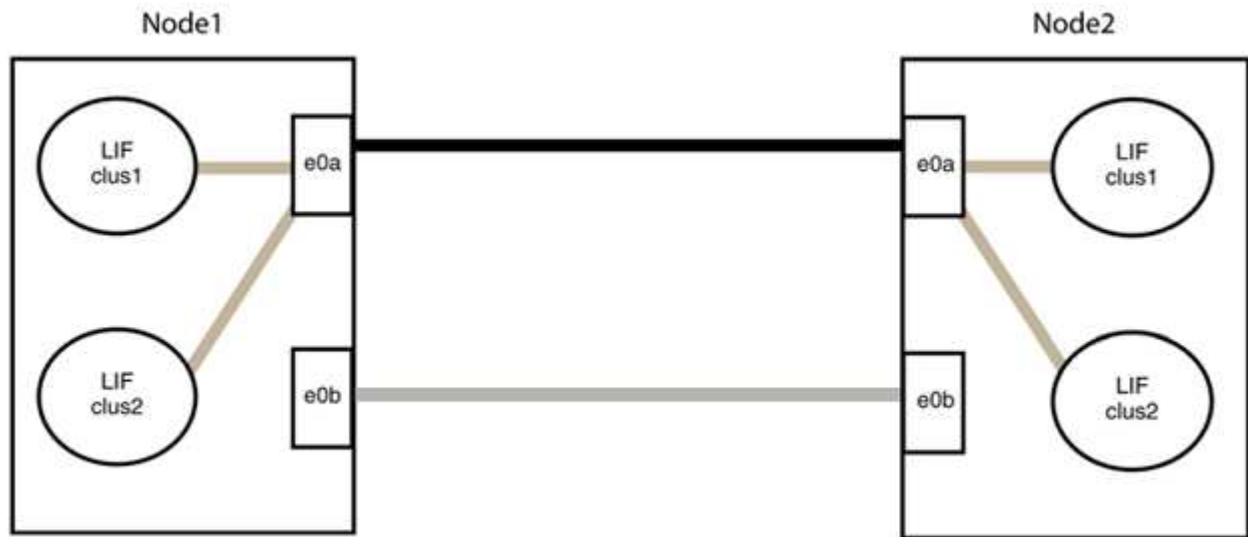
- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

En el ejemplo siguiente, los cables se han desconectado del puerto "e0b" en cada nodo y el tráfico del clúster continúa por la conexión directa entre los puertos "e0a":



b. Conecte los puertos en group2 de vuelta a back.

En el ejemplo siguiente, hay conectado "e0a" en el nodo 1 a "e0a" en el nodo 2 y "e0b" en el nodo 1 está conectado a "e0b" en el nodo 2:



Paso 3: Verificar la configuración

1. Compruebe que los puertos de ambos nodos están conectados correctamente:

```
network device-discovery show -port cluster_port
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster «e0a» y «e0b» están conectados correctamente al puerto correspondiente del partner de clúster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
           e0a     node2                      e0a        AFF-A300
           e0b     node2                      e0b        AFF-A300
node1/lldp
           e0a     node2 (00:a0:98:da:16:44) e0a        -
           e0b     node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a     node1                      e0a        AFF-A300
           e0b     node1                      e0b        AFF-A300
node2/lldp
           e0a     node1 (00:a0:98:da:87:49) e0a        -
           e0b     node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Volver a habilitar la reversión automática para las LIF del clúster:

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

3. Compruebe que todas las LIF son Home. Esto puede tardar unos segundos.

```
network interface show -vserver Cluster -lif lif_name
```

Muestra el ejemplo

Los LIF se han revertido si la columna “es de inicio” es true, como se muestra para node1_clus2 y.. node2_clus2 en el siguiente ejemplo:

```
cluster::> network interface show -vserver Cluster -fields curr-  
port,is-home  
vserver  lif                curr-port is-home  
-----  
Cluster  node1_clus1        e0a      true  
Cluster  node1_clus2        e0b      true  
Cluster  node2_clus1        e0a      true  
Cluster  node2_clus2        e0b      true  
4 entries were displayed.
```

Si alguna LIFS de cluster no ha regresado a sus puertos de directorio raíz, revierta manualmente desde el nodo local:

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

4. Compruebe el estado del clúster de los nodos desde la consola del sistema de cualquier nodo:

```
cluster show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra *epsilon* en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Confirme la conectividad entre los puertos del clúster:

```
cluster ping-cluster local
```

6. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

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

Para obtener más información, consulte ["Artículo de la base de conocimientos de NetApp 1010449: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#).

7. Vuelva a cambiar el nivel de privilegio a admin:


```
set -privilege admin
```

Cisco Nexus 92300YC

Descripción general

Información general de la instalación y configuración para switches Cisco Nexus 92300YC

Antes de configurar los switches Cisco Nexus 92300YC, revise la descripción general del procedimiento.

Para configurar inicialmente un switch Cisco Nexus 92300YC en sistemas que ejecutan ONTAP, siga estos pasos:

1. ["Complete la hoja de trabajo para el cableado Cisco Nexus 92300YC"](#). La hoja de cálculo de cableado de ejemplo proporciona ejemplos de asignaciones de puertos recomendadas desde los switches a las controladoras. La hoja de datos en blanco proporciona una plantilla que puede utilizar para configurar su clúster.
2. ["Configure el switch Cisco Nexus 92300YC"](#). Configure y configure el switch Cisco Nexus 92300YC.
3. ["Preparar la instalación del software NX-OS y del archivo de configuración de referencia \(RCF\)"](#). Prepare la instalación del software NX-OS y del archivo de configuración de referencia (RCF).
4. ["Instale el software NX-OS"](#). Instale el software NX-OS en el switch Nexus 92300YC. NX-OS es un sistema operativo de red para la serie Nexus de switches Ethernet y la serie MDS de switches de red de área de almacenamiento Fibre Channel (FC) proporcionados por Cisco Systems.
5. ["Instalación del archivo de configuración de referencia \(RCF\)"](#). Instale el RCF después de configurar por primera vez el interruptor Nexus 92300YC. También puede utilizar este procedimiento para actualizar la versión de RCF.
6. ["Instale el archivo de configuración del Monitor de estado del conmutador de clúster \(CSHM\)"](#). Instale el archivo de configuración correspondiente para la supervisión del estado del switch del clúster de los switches de clúster Nexus 92300YC.

Información adicional

Antes de iniciar la instalación o el mantenimiento, asegúrese de revisar lo siguiente:

- ["Requisitos de configuración"](#)
- ["Componentes y números de pieza"](#)
- ["Documentación requerida"](#)
- ["Requisitos de Smart Call Home"](#)

Requisitos de configuración para switches Cisco Nexus 92300YC

Para la instalación y el mantenimiento del switch Cisco Nexus 92300YC, asegúrese de revisar todos los requisitos de configuración y red.

Si desea crear clústeres de ONTAP con más de dos nodos, necesita dos switches de red de clúster compatibles. Puede usar switches de gestión adicionales, que son opcionales.

Requisitos de configuración

Para configurar el clúster, necesita el número y el tipo de cables y conectores de cable adecuados para los switches. Según el tipo de switch que esté configurando inicialmente, debe conectarse al puerto de la consola del switch con el cable de consola incluido; también debe proporcionar información de red específica.

Requisitos de red

Necesita la siguiente información de red para todas las configuraciones de los switches:

- Subred IP para el tráfico de red de gestión
- Nombres de host y direcciones IP para cada una de las controladoras del sistema de almacenamiento y todos los switches aplicables
- La mayoría de las controladoras del sistema de almacenamiento se gestionan a través de la interfaz e0M mediante la conexión al puerto de servicio Ethernet (icono de llave inglesa). En los sistemas A800 y A700 de AFF de AFF, la interfaz e0M utiliza un puerto Ethernet dedicado.

Consulte la ["Hardware Universe"](#) para obtener la información más reciente.

Componentes para switches Cisco Nexus 92300YC

Para la instalación y mantenimiento del switch Cisco Nexus 92300YC, asegúrese de revisar todos los componentes del switch y sus números de pieza. Consulte ["Hardware Universe"](#) para obtener más detalles.

En la siguiente tabla se enumeran el número de pieza y la descripción del conmutador 92300YC, los ventiladores y las fuentes de alimentación:

Número de pieza	Descripción
190003	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PTSX (PTSX = escape lateral de puerto)
190003R	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PSIN (PSIN = entrada lateral de puerto)
X-NXA-FAN-35CFM-B	Ventilador, flujo de aire de admisión lateral del puerto Cisco N9K
X-NXA-FAN-35CFM-F	Ventilador, flujo de aire de escape lateral del puerto Cisco N9K
X-NXA-PAC-650W-B.	Fuente de alimentación, Cisco 650W - entrada lateral de puerto
X-NXA-PAC-650W-F	Fuente de alimentación, Cisco 650W - salida lateral de puerto

Detalles del flujo de aire del switch Cisco Nexus 92300YC:

- Flujo de aire de escape del lado del puerto (aire estándar) — el aire frío entra en el chasis a través del ventilador y los módulos de alimentación del pasillo frío y sale por el extremo del puerto del chasis en el pasillo caliente. Flujo de aire de escape del puerto con coloración azul.
- Flujo de aire de admisión del lado del puerto (aire de retroceso) — el aire frío entra en el chasis a través

del extremo del puerto en el pasillo frío y sale por los módulos de ventilador y fuente de alimentación del pasillo caliente. Flujo de aire de entrada en el puerto con colorante borgoña.

Requisitos de documentación para los switches Cisco Nexus 92300YC

Para la instalación y mantenimiento del switch Cisco Nexus 92300YC, asegúrese de revisar toda la documentación recomendada.

Documentación de los switches

Para configurar los switches Cisco Nexus 92300YC, necesita la siguiente documentación de ["Compatibilidad con los 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 acerca de los requisitos del sitio, detalles del switch de hardware y las opciones de instalación.
<i>Guías de configuración del software del switch Cisco Nexus serie 9000</i> (elija la guía para la versión NX-OS instalada en los switches)	Proporciona la información inicial de configuración del switch que necesita para poder configurar el switch para el funcionamiento de ONTAP.
<i>Guía de actualización y degradación de software NX-OS de Cisco Nexus 9000 Series</i> (elija la guía para la versión de NX-OS instalada en los switches)	Proporciona información sobre cómo degradar el switch a software de switch compatible con ONTAP, si es necesario.
<i>Cisco Nexus 9000 Series NX-OS Command Reference Master Index</i>	Proporciona vínculos a las diferentes referencias de comandos proporcionadas por Cisco.
<i>Cisco Nexus 9000 MIBs Reference</i>	Describe los archivos de la base de datos de información de gestión (MIB) para los switches Nexus 9000.
<i>Referencia de mensajes del sistema NX-OS serie Nexus 9000</i>	Describe los mensajes del sistema de los switches Cisco Nexus serie 9000, los 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 Cisco Nexus serie 9000 NX-OS</i> (elija las notas para la versión de NX-OS instalada en los switches)	Describe las funciones, errores y limitaciones de Cisco Nexus 9000 Series.
Cumplimiento normativo e información de seguridad para Cisco Nexus serie 9000	Proporciona información legal, de seguridad y cumplimiento de normativas de agencias 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 desde la ["Centro de documentación de ONTAP 9"](#).

Nombre	Descripción
Específicos del controlador <i>instrucciones de instalación y configuración</i>	Describe cómo instalar el hardware de NetApp.
Documentación de ONTAP	Proporciona información detallada sobre todos los aspectos de las versiones de ONTAP.
"Hardware Universe"	Ofrece información de compatibilidad y configuración de hardware de NetApp.

Kit de raíl y documentación del armario

Para instalar un switch Cisco Nexus 92300YC en un armario NetApp, consulte la siguiente documentación de hardware.

Nombre	Descripción
"Armario del sistema 42U, guía detallada"	Describe las FRU asociadas al armario del sistema 42U, y proporciona instrucciones de mantenimiento y sustitución de FRU.
"[Instale un switch Cisco Nexus 92300YC en un armario de NetApp]"	Describe cómo instalar un switch Cisco Nexus 92300YC en un armario rack de NetApp de cuatro puestos.

Requisitos de Smart Call Home

Para utilizar la función de inicio de llamada inteligente, revise las siguientes directrices.

Smart Call Home supervisa los componentes de hardware y software de su red. Cuando se produce una configuración de sistema crítica, genera una notificación basada en correo electrónico y genera una alerta a todos los destinatarios que están configurados en el perfil de destino. 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 el conmutador de red de clúster para aprovechar la función integrada de soporte Smart Call Home de Cisco.

Antes de poder utilizar Smart Call Home, tenga en cuenta las siguientes consideraciones:

- Debe haber un servidor de correo electrónico.
- El switch debe tener conectividad IP con el servidor de correo electrónico.
- Se debe configurar el nombre del contacto (contacto del servidor SNMP), el número de teléfono y la dirección de la calle. Esto es necesario para determinar el origen de los mensajes recibidos.
- Un ID de CCO debe estar asociado con un contrato de servicio Cisco SMARTnet adecuado para su empresa.

- El servicio Cisco SMARTnet debe estar en su lugar para que el dispositivo se registre.

La ["Sitio de soporte de Cisco"](#) Contiene información acerca de los comandos para configurar Smart Call Home.

Instale el hardware

Complete la hoja de trabajo para el cableado Cisco Nexus 92300YC

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

La hoja de cálculo de cableado de ejemplo proporciona ejemplos de asignaciones de puertos recomendadas desde los switches a las controladoras. La hoja de datos en blanco proporciona una plantilla que puede utilizar para configurar su clúster.

Hoja de trabajo para el cableado de muestra

La definición de puerto de ejemplo de cada par de conmutadores es la siguiente:

Switch de clúster a		Switch del clúster B	
Puerto del switch	Uso de nodos y puertos	Puerto del switch	Uso de nodos y puertos
1	Nodo de 10/25 GbE	1	Nodo de 10/25 GbE
2	Nodo de 10/25 GbE	2	Nodo de 10/25 GbE
3	Nodo de 10/25 GbE	3	Nodo de 10/25 GbE
4	Nodo de 10/25 GbE	4	Nodo de 10/25 GbE
5	Nodo de 10/25 GbE	5	Nodo de 10/25 GbE
6	Nodo de 10/25 GbE	6	Nodo de 10/25 GbE
7	Nodo de 10/25 GbE	7	Nodo de 10/25 GbE
8	Nodo de 10/25 GbE	8	Nodo de 10/25 GbE
9	Nodo de 10/25 GbE	9	Nodo de 10/25 GbE
10	Nodo de 10/25 GbE	10	Nodo de 10/25 GbE
11	Nodo de 10/25 GbE	11	Nodo de 10/25 GbE
12	Nodo de 10/25 GbE	12	Nodo de 10/25 GbE
13	Nodo de 10/25 GbE	13	Nodo de 10/25 GbE

Switch de clúster a		Switch del clúster B	
14	Nodo de 10/25 GbE	14	Nodo de 10/25 GbE
15	Nodo de 10/25 GbE	15	Nodo de 10/25 GbE
16	Nodo de 10/25 GbE	16	Nodo de 10/25 GbE
17	Nodo de 10/25 GbE	17	Nodo de 10/25 GbE
18	Nodo de 10/25 GbE	18	Nodo de 10/25 GbE
19	Nodo de 10/25 GbE	19	Nodo de 10/25 GbE
20	Nodo de 10/25 GbE	20	Nodo de 10/25 GbE
21	Nodo de 10/25 GbE	21	Nodo de 10/25 GbE
22	Nodo de 10/25 GbE	22	Nodo de 10/25 GbE
23	Nodo de 10/25 GbE	23	Nodo de 10/25 GbE
24	Nodo de 10/25 GbE	24	Nodo de 10/25 GbE
25	Nodo de 10/25 GbE	25	Nodo de 10/25 GbE
26	Nodo de 10/25 GbE	26	Nodo de 10/25 GbE
27	Nodo de 10/25 GbE	27	Nodo de 10/25 GbE
28	Nodo de 10/25 GbE	28	Nodo de 10/25 GbE
29	Nodo de 10/25 GbE	29	Nodo de 10/25 GbE
30	Nodo de 10/25 GbE	30	Nodo de 10/25 GbE
31	Nodo de 10/25 GbE	31	Nodo de 10/25 GbE
32	Nodo de 10/25 GbE	32	Nodo de 10/25 GbE
33	Nodo de 10/25 GbE	33	Nodo de 10/25 GbE
34	Nodo de 10/25 GbE	34	Nodo de 10/25 GbE
35	Nodo de 10/25 GbE	35	Nodo de 10/25 GbE

Switch de clúster a		Switch del clúster B	
36	Nodo de 10/25 GbE	36	Nodo de 10/25 GbE
37	Nodo de 10/25 GbE	37	Nodo de 10/25 GbE
38	Nodo de 10/25 GbE	38	Nodo de 10/25 GbE
39	Nodo de 10/25 GbE	39	Nodo de 10/25 GbE
40	Nodo de 10/25 GbE	40	Nodo de 10/25 GbE
41	Nodo de 10/25 GbE	41	Nodo de 10/25 GbE
42	Nodo de 10/25 GbE	42	Nodo de 10/25 GbE
43	Nodo de 10/25 GbE	43	Nodo de 10/25 GbE
44	Nodo de 10/25 GbE	44	Nodo de 10/25 GbE
45	Nodo de 10/25 GbE	45	Nodo de 10/25 GbE
46	Nodo de 10/25 GbE	46	Nodo de 10/25 GbE
47	Nodo de 10/25 GbE	47	Nodo de 10/25 GbE
48	Nodo de 10/25 GbE	48	Nodo de 10/25 GbE
49	Nodo de 40/100 GbE	49	Nodo de 40/100 GbE
50	Nodo de 40/100 GbE	50	Nodo de 40/100 GbE
51	Nodo de 40/100 GbE	51	Nodo de 40/100 GbE
52	Nodo de 40/100 GbE	52	Nodo de 40/100 GbE
53	Nodo de 40/100 GbE	53	Nodo de 40/100 GbE
54	Nodo de 40/100 GbE	54	Nodo de 40/100 GbE
55	Nodo de 40/100 GbE	55	Nodo de 40/100 GbE
56	Nodo de 40/100 GbE	56	Nodo de 40/100 GbE
57	Nodo de 40/100 GbE	57	Nodo de 40/100 GbE

Switch de clúster a		Switch del clúster B	
58	Nodo de 40/100 GbE	58	Nodo de 40/100 GbE
59	Nodo de 40/100 GbE	59	Nodo de 40/100 GbE
60	Nodo de 40/100 GbE	60	Nodo de 40/100 GbE
61	Nodo de 40/100 GbE	61	Nodo de 40/100 GbE
62	Nodo de 40/100 GbE	62	Nodo de 40/100 GbE
63	Nodo de 40/100 GbE	63	Nodo de 40/100 GbE
64	Nodo de 40/100 GbE	64	Nodo de 40/100 GbE
65	ISL de 100 GbE al puerto 65 del switch B.	65	ISL de 100 GbE para cambiar el puerto 65
66	ISL de 100 GbE al puerto 66 del switch B.	66	ISL de 100 GbE para cambiar el puerto 65

Hoja de trabajo de cableado en blanco

Puede utilizar la hoja de datos de cableado vacía para documentar las plataformas que se admiten como nodos de un clúster. La sección *Cluster Connections* del "[Hardware Universe](#)" define los puertos de clúster que utiliza la plataforma.

Switch de clúster a		Switch del clúster B	
Puerto del switch	Uso del nodo/puerto	Puerto del switch	Uso del nodo/puerto
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	

Switch de clúster a		Switch del clúster B	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	

Switch de clúster a		Switch del clúster B	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	
37		37	
38		38	
39		39	
40		40	
41		41	
42		42	
43		43	
44		44	
45		45	
46		46	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	

Switch de clúster a		Switch del clúster B	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	
64		64	
65	ISL al puerto 65 del switch B.	65	ISL para cambiar al puerto 65
66	ISL al puerto 66 del switch B.	66	ISL para cambiar al puerto 66

Configure el switch Cisco Nexus 92300YC

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

Pasos

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

- control de flujo: ninguno

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

Aparecerá la configuración de la cuenta de administración del sistema.

Muestra el ejemplo

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

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

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

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

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

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

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

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

Muestra el ejemplo

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

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

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

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

8. Cree otra cuenta de inicio de sesión:

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

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

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

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

10. Configure el nombre del switch del clúster:

Enter the switch name : **cs2**

11. Configure la interfaz de gestión fuera de banda:

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

Mgmt0 IPv4 address : 172.22.133.216

Mgmt0 IPv4 netmask : 255.255.224.0

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

IPv4 address of the default gateway : 172.22.128.1
```

12. Configure las opciones avanzadas de IP:

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

13. Configurar servicios Telnet:

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

14. Configure los servicios SSH y las claves SSH:

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

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

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

15. Configurar otras opciones:

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

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

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

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

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

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

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

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

El futuro

"[Prepárese para instalar el software NX-OS y RCF](#)".

Revise las consideraciones sobre el cableado y la configuración

Antes de configurar el switch Cisco 92300YC, revise las siguientes consideraciones.

Compatibilidad con los puertos NVIDIA CX6, CX6-DX y Ethernet de CX7 Gb

Si se conecta un puerto de switch a un controlador ONTAP mediante los puertos NIC NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) o ConnectX-7 (CX7), debe codificar de forma fija la velocidad del puerto del switch.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Consulte "[Hardware Universe](#)" para obtener más información sobre los puertos de switch.

Configurar el software

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

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

Lo que necesitará

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

Acerca de los ejemplos

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

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

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

Acerca de esta tarea

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

Pasos

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

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

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

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

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



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

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

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

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

Muestra el ejemplo

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

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

4 entries were displayed.

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

a. Mostrar los atributos del puerto de red: `network port show -ip space Cluster`

Muestra el ejemplo

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

Node: node2

Health					Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						
-----	-----	-----	-----	----	----	-----

e0a	Cluster	Cluster		up	9000	auto/10000
healthy						
e0b	Cluster	Cluster		up	9000	auto/10000
healthy						

Node: node1

Health					Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						
-----	-----	-----	-----	----	----	-----

e0a	Cluster	Cluster		up	9000	auto/10000
healthy						
e0b	Cluster	Cluster		up	9000	auto/10000
healthy						

4 entries were displayed.

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

Muestra el ejemplo

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

4 entries were displayed.

5. Haga ping en las LIF de clúster remoto:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

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

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

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

6. Compruebe que el comando de reversión automática está habilitado en todas las LIF del clúster:

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

Muestra el ejemplo

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

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

4 entries were displayed.

7. Para ONTAP 9.4 y versiones posteriores, habilite la función de recogida de registros de control de estado del switch de clúster para recoger archivos de registro relacionados con el switch mediante los comandos:

```
system cluster-switch log setup-passwordy..system cluster-switch log enable-collection
```

Muestra el ejemplo

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

El futuro

"Instale el software NX-OS".

Instale el software NX-OS

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

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

Revise los requisitos

Puertos y conexiones de nodo compatibles

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

Lo que necesitará

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

Instale el software

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

Acerca de los ejemplos

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

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

Consulte "[Hardware Universe](#)" para los puertos de clúster reales compatibles con la plataforma.

Pasos

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

Muestra el ejemplo

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

```
cs2# ping 172.19.2.1  
Pinging 172.19.2.1 with 0 bytes of data:  
  
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

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

Muestra el ejemplo

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

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

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

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

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

```
show version
```

Muestra el ejemplo

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

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

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

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

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

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

5. Instale la imagen NX-OS.

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

Muestra el ejemplo

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

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

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

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

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

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

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

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

Compatibility check is done:

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

Images will be upgraded according to following table:

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

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

```
Install is in progress, please wait.
```

```
Performing runtime checks.  
[] 100% -- SUCCESS
```

```
Setting boot variables.  
[] 100% -- SUCCESS
```

```
Performing configuration copy.  
[] 100% -- SUCCESS
```

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

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

```
show version
```

Muestra el ejemplo

```
cs2# show version
```

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

Software

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

Hardware

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

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

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

Reason: Reset due to upgrade

System version: 9.2(1)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

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

Muestra el ejemplo

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

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

```
cs2# install epld bootflash:n9000-epld.9.2.2.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	IO FPGA	Successful

1 SUP Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

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

Muestra el ejemplo

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

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

El futuro

["Instale el archivo de configuración de referencia"](#)

Instalación del archivo de configuración de referencia (RCF)

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

Acerca de esta tarea

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

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



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

Pasos

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

Muestra el ejemplo

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

2. Compruebe el estado administrativo y operativo de cada puerto del clúster.
 - a. Compruebe que todos los puertos del clúster tengan el estado correcto: `network port show -ipSpace Cluster`

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

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

Muestra el ejemplo

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

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

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

Muestra el ejemplo

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

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

2 entries were displayed.
```

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

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

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

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

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

Muestra el ejemplo

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

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

Muestra el ejemplo

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

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

```
show running-config
```

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



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

a. Limpie la configuración:

Muestra el ejemplo

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

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

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

b. Reinicie el conmutador:

Muestra el ejemplo

```
(cs2)# reload
```

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

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

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

```
cs2# copy tftp: bootflash: vrf management
```

```
Enter source filename: /code/Nexus_92300YC_RCF_v1.0.2.txt
```

```
Enter hostname for the tftp server: 172.19.2.1
```

```
Enter username: user1
```

```
Outbound-ReKey for 172.19.2.1:22
```

```
Inbound-ReKey for 172.19.2.1:22
```

```
user1@172.19.2.1's password:
```

```
tftp> progress
```

```
Progress meter enabled
```

```
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin  
/code/Nexus_92300YC_R 100% 9687 530.2KB/s 00:00
```

```
tftp> exit
```

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

```
Copy complete.
```

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

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

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

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

```
Disabling ssh: as its enabled right now:
```

```
  generating ecdsa key(521 bits).....
```

```
generated ecdsa key
```

```
Enabling ssh: as it has been disabled
```

```
  this command enables edge port type (portfast) by default on all  
interfaces. You
```

```
  should now disable edge port type (portfast) explicitly on switched  
ports leading to hubs,
```

```
  switches and bridges as they may create temporary bridging loops.
```

```
Edge port type (portfast) should only be enabled on ports connected to a  
single
```

```
  host. Connecting hubs, concentrators, switches, bridges, etc... to  
this
```

```
  interface when edge port type (portfast) is enabled, can cause  
temporary bridging loops.
```

```
  Use with CAUTION
```

```
Edge Port Type (Portfast) has been configured on Ethernet1/1 but will  
only
```

```
  have effect when the interface is in a non-trunking mode.
```

```
...
```

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

```
Copy complete.
```

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

```
show running-config
```



```

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

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

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJlRtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #

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

```



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

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

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

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

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

2. Después de comprobar que las versiones de RCF y los ajustes del switch son correctos, copie el archivo `running-config` en el archivo `startup-config`.

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

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

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

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

4. Compruebe el estado de los puertos del clúster en el clúster.
 - a. Compruebe que los puertos `e0d` están en buen estado y en todos los nodos del clúster: `network port show -ip space Cluster`

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

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

Muestra el ejemplo

A large, empty rectangular box with a dashed border, intended for showing an example. The box is light gray and occupies most of the page below the header.

```

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

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

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

2 entries were displayed.

```

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



```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

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

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

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

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

Muestra el ejemplo

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

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

Muestra el ejemplo

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

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

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

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

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

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

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

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

Muestra el ejemplo

```
cs1# *show port-channel summary*
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/65 (P)  Eth1/66 (P)
cs1#
```

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

Muestra el ejemplo

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

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


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

Muestra el ejemplo

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

15. Haga ping en las interfaces de clúster remoto para verificar la conectividad: `cluster ping-cluster -node local`

Muestra el ejemplo

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

Para ONTAP 9.8 y posterior

Para ONTAP 9.8 y versiones posteriores, habilite la función de recogida de registros del control de estado del switch de clúster para recoger archivos de registro relacionados con el switch, mediante los comandos: `system switch ethernet log setup-password y.. system switch ethernet log enable-collection`

Introduzca: `system switch ethernet log setup-password`

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

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

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

```
Enter the switch name: cs1
```

```
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
```

```
Do you want to continue? {y|n}::[n] y
```

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

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

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

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

```
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
```

```
Do you want to continue? {y|n}:: [n] y
```

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

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

Seguido de: `system switch ethernet log enable-collection`

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

```
Do you want to enable cluster log collection for all nodes in the cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```

Para ONTAP 9.4 y posterior

Para ONTAP 9.4 y versiones posteriores, habilite la función de recogida de registros de control de estado del switch de clúster para recoger archivos de registro relacionados con el switch mediante los comandos:

```
system cluster-switch log setup-password y..system cluster-switch log enable-collection
```

Introduzca: `system cluster-switch log setup-password`

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

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

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

```
Enter the switch name: cs1
```

```
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
```

```
Do you want to continue? {y|n}::[n] y
```

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

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

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

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

```
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
```

```
Do you want to continue? {y|n}:: [n] y
```

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

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

Seguido de: `system cluster-switch log enable-collection`

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

```
Do you want to enable cluster log collection for all nodes in the  
cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

Recopilación de registro de supervisión del estado del switch Ethernet

El monitor de estado del switch Ethernet (CSHM) es responsable de garantizar el estado operativo de los conmutadores de red del clúster y de almacenamiento y de recopilar registros del switch para fines de depuración. Este procedimiento lo guía a través del proceso de configuración e inicio de la recopilación de registros detallados de **Soporte** desde el switch e inicia una recopilación por hora de datos **Periódicos** que es recopilada por AutoSupport.

Pasos

1. Para configurar la recopilación de registros, ejecute el siguiente comando para cada conmutador. Se le pedirá que introduzca el nombre del switch, el nombre de usuario y la contraseña para la recopilación de registros.

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

Muestra el ejemplo

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

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

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

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

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

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

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

2. Para iniciar la recopilación de registros, ejecute el siguiente comando, sustituyendo EL DISPOSITIVO por el conmutador utilizado en el comando anterior. Esto inicia ambos tipos de recopilación de registros: Los registros detallados de **Support** y una recopilación horaria de datos **Periódicos**.

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

Muestra el ejemplo

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Espere 10 minutos y compruebe que se complete la recopilación de registros:

```
system switch ethernet log show
```



Si alguno de estos comandos devuelve un error o si la recogida de registros no se completa, póngase en contacto con el soporte de NetApp.

Solucionar problemas

Si se encuentra con alguno de los siguientes estados de error informados por la función de recopilación de registros (visible en la salida de `system switch ethernet log show`), pruebe los pasos de depuración correspondientes:

Estado de error de recopilación de registros	Resolución
Las claves RSA no están presentes	Vuelva a generar las claves SSH de ONTAP. Póngase en contacto con el soporte de NetApp.
error de contraseña de cambio	Verifique las credenciales, pruebe la conectividad SSH y vuelva a generar las claves SSH de ONTAP. Revise la documentación del switch o póngase en contacto con el soporte de NetApp para obtener instrucciones.
Las claves ECDSA no están presentes para FIPS	Si el modo FIPS está activado, es necesario generar claves ECDSA en el conmutador antes de volver a intentarlo.

registro preexistente encontrado	Elimine el archivo de recopilación de registros anterior del conmutador.
error de registro de volcado del interruptor	Asegúrese de que el usuario del conmutador tiene permisos de recopilación de registros. Consulte los requisitos previos anteriores.

Configurar SNMPv3

Siga este procedimiento para configurar SNMPv3, que admite la monitorización del estado del switch Ethernet (CSHM).

Acerca de esta tarea

Los siguientes comandos configuran un nombre de usuario SNMPv3 en switches Cisco 92300YC:

- Para **sin autenticación**: `snmp-server user SNMPv3_USER NoAuth`
- Para **autenticación MD5/SHA**: `snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD`
- Para autenticación **MD5/SHA con cifrado AES/DES**: `snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv aes-128 PRIV-PASSWORD`

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP: `cluster1::*> security login create -user-or-group-name SNMPv3_USER -application snmp -authentication-method usm -remote-switch-ipaddress ADDRESS`

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM: `cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3 -community-or-username SNMPv3_USER`

Pasos

1. Configure el usuario SNMPv3 en el conmutador para que utilice autenticación y cifrado:

```
show snmp user
```


Muestra el ejemplo

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1) (Config)# show snmp user

-----
-----
                               SNMP USERS
-----
-----

User              Auth              Priv(enforce)    Groups
acl_filter
-----
-----
admin             md5              des(no)          network-admin
SNMPv3User        md5              aes-128(no)      network-operator
-----
-----

NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

User              Auth              Priv
-----
-----

(sw1) (Config)#
```

2. Configure el usuario SNMPv3 en el lado ONTAP:

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

Muestra el ejemplo

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configure CSHM para monitorizar con el nuevo usuario de SNMPv3:

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

Muestra el ejemplo

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

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

Cluster/HA/RDMA

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

4. Compruebe que el número de serie que se va a consultar con el usuario SNMPv3 recién creado es el mismo que se detalla en el paso anterior después de que se haya completado el período de sondeo de CSHM.

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

Muestra el ejemplo

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

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

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

Cluster/HA/RDMA

cluster1::*>
```

Migrar switches

Migre a un clúster con switches de dos nodos con un switch Cisco Nexus 92300YC

Si tiene un entorno de clúster *sin switch* de dos nodos existente, puede migrar a un entorno de clúster *con switches* de dos nodos utilizando switches Cisco Nexus 92300YC para permitirle escalar más allá de los dos nodos del clúster.

El procedimiento que utilice dependerá de si tiene dos puertos de red de clúster dedicados en cada controladora o un único puerto de clúster de cada controladora. El proceso documentado funciona para todos los nodos utilizando puertos ópticos o de twinax; pero no es compatible con este switch si los nodos están usando puertos 10 GB BASE-T RJ45 integrados para los puertos de red del clúster.

La mayoría de los sistemas requieren dos puertos de red de clúster dedicados en cada controladora.



Una vez finalizada la migración, es posible que necesite instalar el archivo de configuración necesario para admitir el Monitor de estado del conmutador de clúster (CSHM) para los conmutadores de clúster 92300YC. Consulte ["Instalación del monitor de estado del interruptor del clúster \(CSHM\)"](#).

Revise los requisitos

Lo que necesitará

En el caso de una configuración sin switch de dos nodos, asegúrese de que:

- La configuración sin switch de dos nodos está correctamente configurada y funciona.
- Los nodos ejecutan ONTAP 9.6 y versiones posteriores.
- Todos los puertos del clúster están en el estado **up**.
- Todas las interfaces lógicas de cluster (LIF) están en el estado **up** y en sus puertos de inicio.

Para la configuración del switch Cisco Nexus 92300YC:

- Ambos switches tienen conectividad de red de gestión.
- Hay acceso de la consola a los switches de clúster.
- El switch de nodo a nodo y las conexiones de switch a switch Nexus 92300YC utilizan cables twinax o fibra.

["Hardware Universe - interruptores"](#) contiene más información sobre el cableado.

- Los cables de enlace entre switches (ISL) están conectados a los puertos 1/65 y 1/66 en los dos switches 92300YC.
- Se ha completado la personalización inicial de los dos conmutadores 92300YC. Para que:
 - Los conmutadores 92300YC están ejecutando la última versión del software
 - Los archivos de configuración de referencia (RCF) se aplican a los conmutadores cualquier personalización del sitio, como SMTP, SNMP y SSH, está configurada en los nuevos conmutadores.

Migrar el switch

Acerca de los ejemplos

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

- Los nombres de los conmutadores 92300YC son cs1 y cs2.
- Los nombres de las SVM del clúster son 1 y 2.
- Los nombres de las LIF son 1_clus1 y 1_clus2 en el nodo 1, y 2_clus1 y 2_clus2 en el nodo 2, respectivamente.
- La `cluster1: :*>` prompt indica el nombre del clúster.
- Los puertos de clúster utilizados en este procedimiento son e0a y e0b.

["Hardware Universe"](#) contiene la información más reciente acerca de los puertos del clúster reales para las plataformas.

Paso 1: Preparación para la migración

1. Cambie el nivel de privilegio a Advanced, introduzca `y` cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (`*>`) aparece.

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

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

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



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

Muestra el ejemplo

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

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

Paso 2: Configure los cables y los puertos

1. Deshabilite todos los puertos orientados a nodos (no los puertos ISL) en los nuevos switches del clúster cs1 y cs2.

No debe deshabilitar los puertos ISL.

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos 1 a 64 que están orientados al nodo están deshabilitados en el switch cs1:

```
cs1# config  
Enter configuration commands, one per line. End with CNTL/Z.  
cs1(config)# interface e/1-64  
cs1(config-if-range)# shutdown
```

2. Verifique que el ISL y los puertos físicos en el ISL entre los dos switches 92300YC cs1 y cs2 estén en los puertos 1/65 y 1/66:

```
show port-channel summary
```

Muestra el ejemplo

El siguiente ejemplo muestra que los puertos ISL están activos en el switch cs1:

```
cs1# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lACP mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/65 (P)  Eth1/66 (P)
```

+ el siguiente ejemplo muestra que los puertos ISL están activos en el conmutador cs2 :

+

```
(cs2)# show port-channel summary
```

```
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lACP mode (member)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/65 (P)  Eth1/66 (P)
```

3. Mostrar la lista de dispositivos vecinos:

```
show cdp neighbors
```

Este comando proporciona información sobre los dispositivos conectados al sistema.

Muestra el ejemplo

En el siguiente ejemplo se enumeran los dispositivos vecinos del conmutador cs1:

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID           Local Intrfce  Hldtme Capability  Platform
Port ID
cs2 (FDO220329V5)   Eth1/65        175    R S I s         N9K-C92300YC
Eth1/65
cs2 (FDO220329V5)   Eth1/66        175    R S I s         N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

+ el siguiente ejemplo enumera los dispositivos vecinos en el conmutador cs2:

+

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID           Local Intrfce  Hldtme Capability  Platform
Port ID
cs1 (FDO220329KU)   Eth1/65        177    R S I s         N9K-C92300YC
Eth1/65
cs1 (FDO220329KU)   Eth1/66        177    R S I s         N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

4. Compruebe que todos los puertos del clúster estén activos:

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

Cada puerto debería mostrarse para Link y saludable para Health Status.

Muestra el ejemplo

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

Node: node1

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

Node: node2

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

4 entries were displayed.

5. Compruebe que todas las LIF del clúster estén en funcionamiento:

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

Cada LIF de clúster debería mostrar el valor true para Is Home y que tengan un Status Admin/Oper de arriba/arriba

Muestra el ejemplo

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			
4 entries were displayed.				

6. Compruebe que la reversión automática está habilitada en todas las LIF del clúster:

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

Muestra el ejemplo

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

	Logical	
Vserver	Interface	Auto-revert

Cluster		
	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true
4 entries were displayed.		

7. Desconecte el cable del puerto e0a del clúster en el nodo 1 y, a continuación, conecte e0a al puerto 1 del switch del clúster cs1 mediante el cableado adecuado compatible con los switches 92300YC.

La "[Hardware Universe - Switches](#)" contiene más información sobre el cableado.

- Desconecte el cable del puerto e0a del clúster en el nodo 2 y, a continuación, conecte e0a al puerto 2 del switch del clúster cs1 con el cableado adecuado compatible con los switches 92300YC.
- Habilite todos los puertos orientados al nodo en el switch de clúster cs1.

Muestra el ejemplo

El ejemplo siguiente muestra que los puertos 1/1 a 1/64 están habilitados en el conmutador cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-64
cs1(config-if-range)# no shutdown
```

- Compruebe que todos los LIF del clúster estén activos, operativos y se muestren como true para Is Home:

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

Muestra el ejemplo

En el ejemplo siguiente, se muestra que todas las LIF están activas en los nodos 1 y 2, y eso Is Home los resultados son verdaderos:

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

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

4 entries were displayed.

11. Muestra información sobre el estado de los nodos en el clúster:

```
cluster show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra información sobre el estado y la elegibilidad de los nodos en el clúster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1	true	true	false
node2	true	true	false

```
2 entries were displayed.
```

12. Desconecte el cable del puerto e0b del clúster en el nodo 1 y, a continuación, conecte e0b al puerto 1 del switch cs2 del clúster mediante el cableado adecuado compatible con los switches 92300YC.
13. Desconecte el cable del puerto e0b del clúster en el nodo 2 y, a continuación, conecte e0b al puerto 2 del switch del clúster cs2 mediante el cableado adecuado compatible con los switches 92300YC.
14. Habilite todos los puertos orientados al nodo en el switch de clúster cs2.

Muestra el ejemplo

El ejemplo siguiente muestra que los puertos 1/1 a 1/64 están habilitados en el conmutador cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-64
cs2(config-if-range)# no shutdown
```

Paso 3: Verificar la configuración

1. Compruebe que todos los puertos del clúster estén activos:

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

Muestra el ejemplo

En el siguiente ejemplo, se muestra que todos los puertos del clúster están en los nodos 1 y 2:

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

Node: node1

Ignore

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

Node: node2

Ignore

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

4 entries were displayed.

2. Compruebe que todas las interfaces muestran true for Is Home:

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



Esto puede tardar varios minutos en completarse.

Muestra el ejemplo

En el ejemplo siguiente, se muestra que todas las LIF están activas en los nodos 1 y 2, y eso Is Home los resultados son verdaderos:

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

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

4 entries were displayed.

3. Compruebe que ambos nodos tengan una conexión cada uno con cada switch:

```
show cdp neighbors
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran los resultados adecuados para ambos switches:


```
(cs1)# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	133	H	FAS2980
node2 e0a	Eth1/2	133	H	FAS2980
cs2(FDO220329V5) Eth1/65	Eth1/65	175	R S I s	N9K-C92300YC
cs2(FDO220329V5) Eth1/66	Eth1/66	175	R S I s	N9K-C92300YC

Total entries displayed: 4

```
(cs2)# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	133	H	FAS2980
node2 e0b	Eth1/2	133	H	FAS2980
cs1(FDO220329KU) Eth1/65	Eth1/65	175	R S I s	N9K-C92300YC
cs1(FDO220329KU) Eth1/66	Eth1/66	175	R S I s	N9K-C92300YC

Total entries displayed: 4

4. Muestra información sobre los dispositivos de red detectados en el clúster:

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

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/          Local   Discovered
Protocol       Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node2          /cdp
               e0a    cs1                        0/2      N9K-
C92300YC
               e0b    cs2                        0/2      N9K-
C92300YC
node1          /cdp
               e0a    cs1                        0/1      N9K-
C92300YC
               e0b    cs2                        0/1      N9K-
C92300YC

4 entries were displayed.
```

5. Compruebe que la configuración está desactivada:

```
network options switchless-cluster show
```



El comando puede tardar varios minutos en completarse. Espere a que se anuncie la duración de 3 minutos.

Muestra el ejemplo

El resultado falso en el ejemplo siguiente muestra que las opciones de configuración están deshabilitadas:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

6. Compruebe el estado de los miembros del nodo en el clúster:

```
cluster show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra información sobre el estado y la elegibilidad de los nodos en el clúster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1	true	true	false
node2	true	true	false

7. Compruebe que la red de clúster tiene conectividad completa:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

```
cluster1::> cluster ping-cluster -node node2
```

Host is node2

Getting addresses from network interface table...

Cluster node1_clus1 169.254.209.69 node1 e0a

Cluster node1_clus2 169.254.49.125 node1 e0b

Cluster node2_clus1 169.254.47.194 node2 e0a

Cluster node2_clus2 169.254.19.183 node2 e0b

Local = 169.254.47.194 169.254.19.183

Remote = 169.254.209.69 169.254.49.125

Cluster Vserver Id = 4294967293

Ping status:

Basic connectivity succeeds on 4 path(s)

Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):

Local 169.254.47.194 to Remote 169.254.209.69

Local 169.254.47.194 to Remote 169.254.49.125

Local 169.254.19.183 to Remote 169.254.209.69

Local 169.254.19.183 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)

8. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

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

Muestra el ejemplo

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

9. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

10. Para ONTAP 9.4 y versiones posteriores, habilite la función de recogida de registros del control de estado del switch de clúster para recoger archivos de registro relacionados con el switch, mediante los comandos:

```
system cluster-switch log setup-password y..system cluster-switch log enable-  
collection
```

Muestra el ejemplo

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

Migre desde un switch de Cisco a un switch Cisco Nexus 92300YC

Puede migrar switches de clúster Cisco antiguos sin interrupciones para un clúster ONTAP a switches de red de clúster Cisco Nexus 92300YC.



Una vez finalizada la migración, es posible que necesite instalar el archivo de configuración necesario para admitir el Monitor de estado del conmutador de clúster (CSHM) para los conmutadores de clúster 92300YC. Consulte ["Instalación del monitor de estado del interruptor del clúster \(CSHM\)"](#).

Revise los requisitos

Lo que necesitará

- Un clúster existente totalmente funcional.
- Conectividad de 10 GbE y 40 GbE desde los nodos a los switches de clúster Nexus 92300YC
- Todos los puertos del clúster están en estado up para garantizar operaciones no disruptivas.
- Versión correcta de NX-OS y el archivo de configuración de referencia (RCF) instalados en los switches de clúster Nexus 92300YC.
- Un clúster de NetApp redundante y totalmente funcional mediante switches Cisco anteriores.
- Conectividad de la administración y acceso de consola a los switches Cisco anteriores y a los nuevos.
- Todos los LIF del clúster con las LIF del clúster están en sus puertos de inicio.
- Puertos ISL habilitados y cableado entre los switches de Cisco anteriores y entre los switches nuevos.

Migrar el switch

Acerca de los ejemplos

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

- Los switches de clúster existentes de Cisco Nexus 5596UP son c1 y c2.
- Los nuevos switches de clúster Nexus 92300YC son cs1 y cs2.
- Los nodos son 1 y 2.
- Las LIF del clúster son 1_clus1 y 1_clus2 en el nodo 1, y 2_clus1 y 2_clus2 en el nodo 2, respectivamente.
- El interruptor c2 se sustituye primero por el interruptor cs2 y, a continuación, el interruptor c1 se sustituye por el interruptor cs1.
 - Un ISL temporal se basa en cs1 que conecta c1 a cs1.
 - El cableado entre los nodos y c2 se desconecta de c2 y se vuelve a conectar a cs2.
 - El cableado entre los nodos y c1 se desconecta de c1 y se vuelve a conectar a cs1.
 - A continuación, se quita el ISL temporal entre c1 y cs1.

Puertos que se utilizan para conexiones

- Algunos puertos están configurados en switches Nexus 92300YC para que se ejecuten a 10 GbE o 40 GbE.
- Los switches de clúster utilizan los siguientes puertos para las conexiones a los nodos:
 - Puertos e1/1-48 (10/25 GbE), e1/49-64 (40/100 GbE): Nexus 92300YC
 - Puertos e1/1-40 (10 GbE): Nexus 5596UP

- Puertos e1/1-32 (10 GbE): Nexus 5020
- Puertos e1/1-12, e2/1-6 (10 GbE): Nexus 5010 con módulo de expansión
- Los switches de clúster utilizan los siguientes puertos de enlace entre switches (ISL):
 - Puertos e1/65-66 (100 GbE): Nexus 92300YC
 - Puertos e1/41-48 (10 GbE): Nexus 5596UP
 - Puertos e1/33-40 (10 GbE): Nexus 5020
 - Puertos e1/13-20 (10 GbE): Nexus 5010
- ["Hardware Universe - interruptores"](#) contiene información sobre el cableado compatible para todos los switches de clúster.
- Las versiones ONTAP y NX-OS compatibles con este procedimiento son en la ["Switches Ethernet de Cisco"](#) página.

Paso 1: Preparación para la migración

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

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

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

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

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



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

Muestra el ejemplo

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

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

3. Compruebe que la reversión automática está habilitada en todas las LIF del clúster:

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

Muestra el ejemplo

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

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

4 entries were displayed.

4. Determine el estado administrativo u operativo de cada interfaz de clúster:

Cada puerto debería mostrarse para Link y saludable para Health Status.

a. Mostrar los atributos del puerto de red:

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


Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

4 entries were displayed.
```

- b. Muestra información sobre las interfaces lógicas y sus nodos principales designados:

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

Cada LIF debería mostrarse arriba/arriba Status Admin/Oper y fiel para Is Home.

Muestra el ejemplo

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

4 entries were displayed.

5. Compruebe que los puertos del clúster de cada nodo están conectados a los switches de clúster existentes de la siguiente manera (desde la perspectiva de los nodos) mediante el comando:

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

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node2      /cdp
           e0a    c1                        0/2      N5K-
C5596UP
           e0b    c2                        0/2      N5K-
C5596UP
node1      /cdp
           e0a    c1                        0/1      N5K-
C5596UP
           e0b    c2                        0/1      N5K-
C5596UP

4 entries were displayed.
```

6. Compruebe que los puertos y los switches del clúster están conectados de la siguiente manera (desde la perspectiva de los switches) mediante el comando:

```
show cdp neighbors
```

Muestra el ejemplo

```
c1# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	124	H	FAS2750
node2 e0a	Eth1/2	124	H	FAS2750
c2 (FOX2025GEFC) Eth1/41	Eth1/41	179	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/42	Eth1/42	175	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/43	Eth1/43	179	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/44	Eth1/44	175	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/45	Eth1/45	179	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/46	Eth1/46	179	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/47	Eth1/47	175	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/48	Eth1/48	179	S I s	N5K-C5596UP

Total entries displayed: 10

```
c2# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	124	H	FAS2750
node2 e0b	Eth1/2	124	H	FAS2750
c1 (FOX2025GEEX) Eth1/41	Eth1/41	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/42	Eth1/42	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/43	Eth1/43	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/44	Eth1/44	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/45	Eth1/45	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/46	Eth1/46	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/47	Eth1/47	176	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/48	Eth1/48	176	S I s	N5K-C5596UP

7. Compruebe que la red de clúster tiene conectividad completa mediante el comando:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Paso 2: Configure los cables y los puertos

1. Configurar un ISL temporal en los puertos cs1 en e1/41-48, entre c1 y cs1.

Muestra el ejemplo

El siguiente ejemplo muestra cómo se configura el nuevo ISL en c1 y cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/41-48
cs1(config-if-range)# description temporary ISL between Nexus 5596UP
and Nexus 92300YC
cs1(config-if-range)# no lldp transmit
cs1(config-if-range)# no lldp receive
cs1(config-if-range)# switchport mode trunk
cs1(config-if-range)# no spanning-tree bpduguard enable
cs1(config-if-range)# channel-group 101 mode active
cs1(config-if-range)# exit
cs1(config)# interface port-channel 101
cs1(config-if)# switchport mode trunk
cs1(config-if)# spanning-tree port type network
cs1(config-if)# exit
cs1(config)# exit
```

2. Quite los cables ISL de los puertos e1/41-48 de c2 y conecte los cables a los puertos e1/41-48 en cs1.
3. Compruebe que los puertos ISL y el puerto-canal estén operativos conectando c1 y cs1:

```
show port-channel summary
```

Muestra el ejemplo

En el siguiente ejemplo, se muestra el comando de resumen de puerto-canal de Cisco que se está utilizando para verificar que los puertos ISL están operativos en c1 y cs1:

c1# **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      Eth1/41(P)  Eth1/42(P)  
Eth1/43(P)  
Eth1/44(P)  Eth1/45(P)  
Eth1/46(P)  Eth1/47(P)  Eth1/48(P)
```

cs1# **show port-channel summary**

Flags: D - Down P - Up in port-channel (members)
I - Individual H - Hot-standby (LACP only)
s - Suspended r - Module-removed
b - BFD Session Wait
S - Switched R - Routed
U - Up (port-channel)
p - Up in delay-lACP mode (member)
M - Not in use. Min-links not met

```
-----  
-----  
Group Port-      Type      Protocol  Member Ports  
Channel  
-----  
-----  
1      Po1(SU)    Eth      LACP      Eth1/65(P)  Eth1/66(P)  
101    Po101(SU)  Eth      LACP      Eth1/41(P)  Eth1/42(P)  
Eth1/43(P)  
Eth1/44(P)  Eth1/45(P)  
Eth1/46(P)  Eth1/47(P)  Eth1/48(P)
```

4. Para el nodo 1, desconecte el cable de e1/1 en c2 y, a continuación, conecte el cable a e1/1 en cs2, utilizando el cableado adecuado compatible con Nexus 92300YC.
5. Para el nodo 2, desconecte el cable de e1/2 en c2 y, a continuación, conecte el cable a e1/2 en cs2, utilizando el cableado adecuado compatible con Nexus 92300YC.
6. Los puertos de clúster de cada nodo ahora están conectados a los switches de clúster del siguiente modo, desde la perspectiva de los nodos:

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

Muestra el ejemplo

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	c1	0/2	N5K-
C5596UP				
	e0b	cs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	c1	0/1	N5K-
C5596UP				
	e0b	cs2	0/1	N9K-
C92300YC				

4 entries were displayed.

7. Para el nodo 1, desconecte el cable de e1/1 en c1 y, a continuación, conecte el cable a e1/1 en cs1, utilizando el cableado adecuado compatible con Nexus 92300YC.
8. Para el nodo 2, desconecte el cable de e1/2 en c1 y, a continuación, conecte el cable a e1/2 en cs1, utilizando el cableado adecuado compatible con Nexus 92300YC.
9. Los puertos de clúster de cada nodo ahora están conectados a los switches de clúster del siguiente modo, desde la perspectiva de los nodos:

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

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface
Platform
-----
node2      /cdp
           e0a    cs1                      0/2          N9K-
C92300YC
           e0b    cs2                      0/2          N9K-
C92300YC
node1      /cdp
           e0a    cs1                      0/1          N9K-
C92300YC
           e0b    cs2                      0/1          N9K-
C92300YC
4 entries were displayed.
```

10. Elimine el ISL temporal entre cs1 y c1.

Muestra el ejemplo

```
cs1(config)# no interface port-channel 10
cs1(config)# interface e1/41-48
cs1(config-if-range)# lldp transmit
cs1(config-if-range)# lldp receive
cs1(config-if-range)# no switchport mode trunk
cs1(config-if-range)# no channel-group
cs1(config-if-range)# description 10GbE Node Port
cs1(config-if-range)# spanning-tree bpduguard enable
cs1(config-if-range)# exit
cs1(config)# exit
```

Paso 3: Complete la migración

1. Compruebe la configuración final del clúster:

```
network port show -ipSPACE Cluster
```

Cada puerto debería mostrarse para Link y saludable para Health Status.

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

4 entries were displayed.

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			

```

node1_clus2 up/up 169.254.49.125/16 node1
e0b true
node2_clus1 up/up 169.254.47.194/16 node2
e0a true
node2_clus2 up/up 169.254.19.183/16 node2
e0b true

```

4 entries were displayed.

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	cs1	0/2	N9K-
C92300YC				
	e0b	cs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C92300YC				
	e0b	cs2	0/1	N9K-
C92300YC				

4 entries were displayed.

cs1# **show cdp neighbors**

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1	Eth1/1	124	H	FAS2750
e0a				
node2	Eth1/2	124	H	FAS2750
e0a				
cs2 (FD0220329V5)	Eth1/65	179	R S I s	N9K-C92300YC
Eth1/65				

```
cs2(FDO220329V5)      Eth1/66      179      R S I s      N9K-C92300YC
Eth1/66
```

```
cs2# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	124	H	FAS2750
node2 e0b	Eth1/2	124	H	FAS2750
cs1(FDO220329KU) Eth1/65	Eth1/65	179	R S I s	N9K-C92300YC
cs1(FDO220329KU) Eth1/66	Eth1/66	179	R S I s	N9K-C92300YC

Total entries displayed: 4

2. Compruebe que la red de clúster tiene conectividad completa:

```
cluster ping-cluster -node node-name
```

Muestra el ejemplo

```
cluster1::*> set -priv advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by NetApp personnel.

Do you want to continue? {y|n}: **y**

```
cluster1::*> cluster ping-cluster -node node2
```

Host is node2

Getting addresses from network interface table...

Cluster node1_clus1 169.254.209.69 node1 e0a

Cluster node1_clus2 169.254.49.125 node1 e0b

Cluster node2_clus1 169.254.47.194 node2 e0a

Cluster node2_clus2 169.254.19.183 node2 e0b

Local = 169.254.47.194 169.254.19.183

Remote = 169.254.209.69 169.254.49.125

Cluster Vserver Id = 4294967293

Ping status:

....

Basic connectivity succeeds on 4 path(s)

Basic connectivity fails on 0 path(s)

.....

Detected 9000 byte MTU on 4 path(s):

Local 169.254.19.183 to Remote 169.254.209.69

Local 169.254.19.183 to Remote 169.254.49.125

Local 169.254.47.194 to Remote 169.254.209.69

Local 169.254.47.194 to Remote 169.254.49.125

Larger than PMTU communication succeeds on 4 path(s)

RPC status:

2 paths up, 0 paths down (tcp check)

2 paths up, 0 paths down (udp check)

```
cluster1::*> set -privilege admin
```

```
cluster1::*>
```

3. Para ONTAP 9.4 y versiones posteriores, habilite la función de recogida de registros del control de estado del switch de clúster para recoger archivos de registro relacionados con el switch, mediante los comandos:

```
system cluster-switch log setup-password y..system cluster-switch log enable-collection
```

Muestra el ejemplo

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

Sustituya los interruptores

Sustituya un switch Cisco Nexus 92300YC

La sustitución de un switch Nexus 92300YC defectuoso en una red de clúster es un procedimiento no disruptivo (NDU).

Revise los requisitos

Lo que necesitará

Antes de realizar la sustitución del interruptor, asegúrese de que:

- En el clúster y la infraestructura de red existentes:
 - El clúster existente se ha verificado como completamente funcional, con al menos un switch de clúster completamente conectado.
 - Todos los puertos del clúster están activos.
 - Todas las interfaces lógicas de clúster (LIF) están en funcionamiento y en sus puertos raíz.
 - El comando `ONTAP cluster ping-cluster -node no1` debe indicar que la conectividad básica y el tamaño superior que la comunicación PMTU son correctos en todas las rutas.
- Para el switch de sustitución Nexus 92300YC:
 - La conectividad de la red de gestión en el switch de reemplazo es funcional.
 - El acceso de la consola al interruptor de sustitución está en su lugar.
 - Las conexiones de los nodos son los puertos 1/1 a 1/64.
 - Todos los puertos de enlace entre switches (ISL) están deshabilitados en los puertos 1/65 y 1/66.
 - El archivo de configuración de referencia (RCF) y el conmutador de imagen del sistema operativo NX-OS se cargan en el conmutador.
 - Se ha completado la personalización inicial del conmutador, tal como se detalla en: ["Configure el switch Cisco Nexus 92300YC"](#).

Cualquier personalización de sitio anterior, como STP, SNMP y SSH, se copian al nuevo switch.

Sustituya el interruptor

Acerca de los ejemplos

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

- Los nombres de los switches Nexus 92300YC existentes son cs1 y cs2.
- El nombre del nuevo switch Nexus 92300YC es newcs2.
- Los nombres de nodo son 1 y 2.
- Los puertos del clúster de cada nodo se denominan e0a y e0b.
- Los nombres de las LIF del clúster son 1_clus1 y 1_clus2 para los nodos 1, y 2_clus1 y 2_clus2 para los nodos 2.
- El símbolo del sistema de cambios en todos los nodos del cluster es `cluster1:*>`

Acerca de esta tarea

Debe ejecutar el comando para migrar una LIF de clúster desde el nodo donde se aloja la LIF del clúster.

El siguiente procedimiento se basa en la siguiente topología de red de clúster:

Mostrar topologia

cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore						
						Speed(Mbps) Health
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper Status
Status						

e0a	Cluster	Cluster		up	9000	auto/10000 healthy
false						
e0b	Cluster	Cluster		up	9000	auto/10000 healthy
false						

Node: node2

Ignore						
						Speed(Mbps) Health
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper Status
Status						

e0a	Cluster	Cluster		up	9000	auto/10000 healthy
false						
e0b	Cluster	Cluster		up	9000	auto/10000 healthy
false						

4 entries were displayed.

cluster1::*> network interface show -vserver Cluster

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

Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b

```

true
node2_clus1 up/up 169.254.47.194/16 node2 e0a
true
node2_clus2 up/up 169.254.19.183/16 node2 e0b
true
4 entries were displayed.

```

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

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

4 entries were displayed.

```
cs1# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID	Local Intrfce	Hldtme	Capability	Platform	Port
ID					
node1	Eth1/1	144	H	FAS2980	e0a
node2	Eth1/2	145	H	FAS2980	e0a
cs2 (FD0220329V5)	Eth1/65	176	R S I s	N9K-C92300YC	
Eth1/65					
cs2 (FD0220329V5)	Eth1/66	176	R S I s	N9K-C92300YC	
Eth1/66					

Total entries displayed: 4

```
cs2# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID ID	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	139	H	FAS2980	e0b
node2	Eth1/2	124	H	FAS2980	e0b
cs1 (FDO220329KU) Eth1/65	Eth1/65	178	R S I s	N9K-C92300YC	
cs1 (FDO220329KU) Eth1/66	Eth1/66	178	R S I s	N9K-C92300YC	

Total entries displayed: 4

Paso 1: Prepararse para la sustitución

1. Instale el RCF y la imagen adecuados en el interruptor, newcs2, y realice las preparaciones necesarias del sitio.

Si es necesario, verifique, descargue e instale las versiones apropiadas del software RCF y NX-OS para el nuevo switch. Si ha comprobado que el nuevo conmutador está correctamente configurado y no necesita actualizaciones para el software RCF y NX-OS, continúe con el paso 2.

- a. Vaya a la página *NetApp Cluster and Management Network Switches Reference Configuration File Description* en el sitio de soporte de NetApp.
 - b. Haga clic en el vínculo de *Cluster Network and Management Network Compatibility Matrix* y a continuación, anote la versión de software del switch que desee.
 - c. Haga clic en la flecha de retroceso de su navegador para volver a la página **Descripción**, haga clic en **CONTINUAR**, acepte el acuerdo de licencia y, a continuación, vaya a la página **Descargar**.
 - d. Siga los pasos de la página Descarga para descargar los archivos RCF y NX-OS correctos para la versión del software ONTAP que está instalando.
2. En el nuevo switch, inicie sesión como administrador y apague todos los puertos que se conectarán a las interfaces de clúster de nodos (puertos 1/1 a 1/64).

Si el interruptor que va a sustituir no funciona y está apagado, vaya al paso 4. Los LIF de los nodos del clúster ya deberían haber realizado la conmutación al otro puerto del clúster para cada nodo.

Muestra el ejemplo

```
newcs2# config  
Enter configuration commands, one per line. End with CNTL/Z.  
newcs2(config)# interface e1/1-64  
newcs2(config-if-range)# shutdown
```

3. Compruebe que todas las LIF del clúster tengan la reversión automática habilitada:

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

Muestra el ejemplo

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

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

4 entries were displayed.

4. Compruebe que todas las LIF del clúster pueden comunicarse:

```
cluster ping-cluster
```

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster node1

Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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)
```

Paso 2: Configure los cables y los puertos

1. Apague los puertos ISL 1/65 y 1/66 en el switch Nexus 92300YC cs1:

Muestra el ejemplo

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/65-66
cs1(config-if-range)# shutdown
cs1(config-if-range)#
```

2. Retire todos los cables del switch Nexus 92300YC cs2 y, a continuación, conéctelos a los mismos puertos del switch Nexus 92300YC newcs2.

3. Traiga los puertos ISL 1/65 y 1/66 entre los switches cs1 y newcs2 y, a continuación, verifique el estado de operación del canal de puerto.

Port-Channel debe indicar PO1(su) y los puertos de miembro deben indicar eth1/65(P) y eth1/66(P).

Muestra el ejemplo

En este ejemplo, se habilitan los puertos ISL 1/65 y 1/66, y se muestra un resumen de canal de puerto en el switch cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/65-66
cs1(config-if-range)# no shutdown

cs1(config-if-range)# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lACP mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
      Channel
-----
-----
1      Po1 (SU)       Eth      LACP      Eth1/65 (P)  Eth1/66 (P)

cs1(config-if-range)#
```

4. Verifique que el puerto e0b esté activo en todos los nodos:

```
network port show ipspace Cluster
```


Muestra el ejemplo

La salida debe ser similar a la siguiente:

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

Node: node1

Ignore

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

Node: node2

Ignore

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

4 entries were displayed.
```

5. En el mismo nodo que utilizó en el paso anterior, revierte la LIF del clúster asociada con el puerto en el paso anterior usando el comando `network interface revert`.

Muestra el ejemplo

En este ejemplo, la LIF no1_clus2 del nodo 1 se revierte correctamente si el valor Home es TRUE y el puerto es e0b.

Los siguientes comandos devuelven la LIF node1_clus2 encendido node1 al puerto de inicio e0a Y muestra información acerca de las LIF en ambos nodos. La creación del primer nodo se realiza correctamente si la columna es Inicio es true para ambas interfaces del clúster y se muestran las asignaciones de puerto correctas, en este ejemplo e0a y.. e0b en el nodo 1.

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0a	false			

4 entries were displayed.

6. Muestra información sobre los nodos de un clúster:

```
cluster show
```

Muestra el ejemplo

En este ejemplo, se muestra que el estado del nodo para el nodo 1 y el nodo 2 en este clúster es TRUE.

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1	false	true
node2	true	true

7. Compruebe que todos los puertos físicos del clúster estén en funcionamiento:

```
network port show ipspace Cluster
```

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

4 entries were displayed.

Paso 3: Complete el procedimiento

1. Compruebe que todas las LIF del clúster pueden comunicarse:

```
cluster ping-cluster
```

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 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)
```

2. Confirme la siguiente configuración de red del clúster:

```
network port show
```

Muestra el ejemplo

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

```
Node: node1
```

```
Ignore
```

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

```
Node: node2
```

```
Ignore
```

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

```
4 entries were displayed.
```

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

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

```
e0b      true
          node2_clus1  up/up    169.254.47.194/16  node2
e0a      true
          node2_clus2  up/up    169.254.19.183/16  node2
e0b      true
```

4 entries were displayed.

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				
node2	/cdp			
	e0a	cs1	0/2	N9K-
C92300YC				
	e0b	newcs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C92300YC				
	e0b	newcs2	0/1	N9K-
C92300YC				

4 entries were displayed.

```
cs1# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID	Local	Intrfce	Hldtme	Capability	Platform
Port ID					
node1		Eth1/1	144	H	FAS2980
e0a					
node2		Eth1/2	145	H	FAS2980
e0a					
newcs2 (FDO296348FU)		Eth1/65	176	R S I s	N9K-C92300YC
Eth1/65					
newcs2 (FDO296348FU)		Eth1/66	176	R S I s	N9K-C92300YC

Eth1/66

Total entries displayed: 4

cs2# **show cdp neighbors**

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	139	H	FAS2980
node2 e0b	Eth1/2	124	H	FAS2980
cs1 (FDO220329KU) Eth1/65	Eth1/65	178	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	178	R S I s	N9K-C92300YC

Total entries displayed: 4

3. En ONTAP 9.4 y versiones posteriores, habilite la función de recogida de registros del control de estado del switch de clúster para recopilar archivos de registro relacionados con el switch mediante gthe commds:

```
system cluster-switch log setup-passwordy..system cluster-switch log enable-  
collection
```


Muestra el ejemplo

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



Si alguno de estos comandos devuelve un error, póngase en contacto con el soporte de NetApp.

Sustituya los switches de clúster Cisco Nexus 92300YC por conexiones sin switches

Puede migrar desde un clúster con una red de clúster conmutada a uno donde dos nodos están conectados directamente para ONTAP 9.3 y versiones posteriores.

Revise los requisitos

Directrices

Revise las siguientes directrices:

- La migración a una configuración de clúster de dos nodos sin switch es una operación no disruptiva. La mayoría de los sistemas tienen dos puertos de interconexión de clúster dedicados en cada nodo, pero también puede usar este procedimiento para sistemas con un número mayor de puertos de interconexión de clúster dedicados en cada nodo, como cuatro, seis u ocho.
- No se puede usar la función de interconexión de clúster sin switches con más de dos nodos.
- Si tiene un clúster de dos nodos existente que utiliza switches de interconexión de clúster y ejecuta ONTAP 9.3 o una versión posterior, puede reemplazar los switches por conexiones directas de vuelta a atrás entre los nodos.

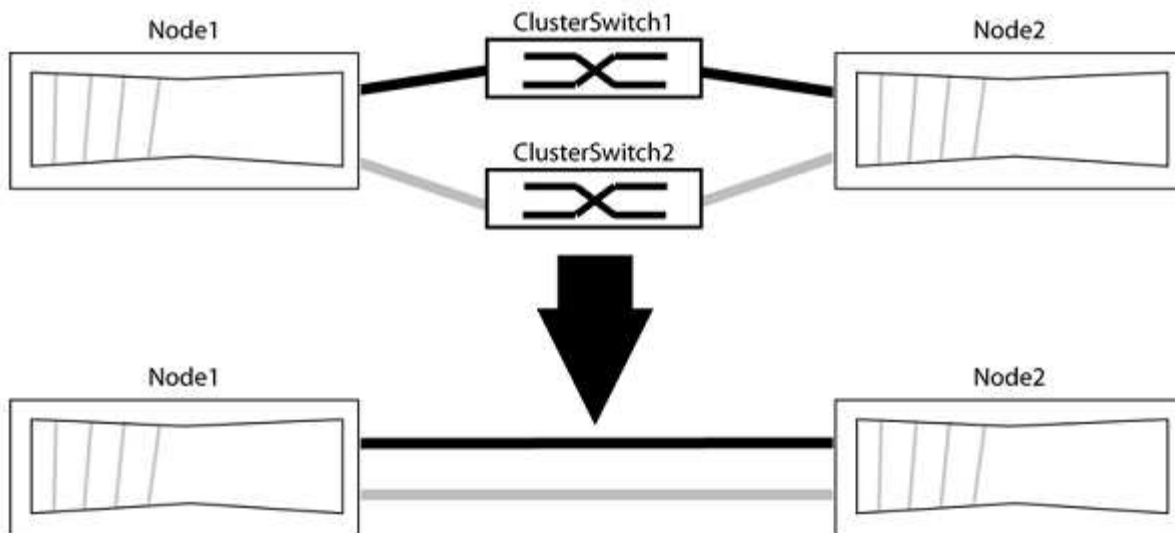
Lo que necesitará

- Un clúster en buen estado que consta de dos nodos conectados por switches de clúster. Los nodos deben ejecutar la misma versión de ONTAP.
- Cada nodo con el número requerido de puertos de clúster dedicados, que proporcionan conexiones redundantes de interconexión de clúster para admitir la configuración de su sistema. Por ejemplo, hay dos puertos redundantes para un sistema con dos puertos de Cluster Interconnect dedicados en cada nodo.

Migrar los switches

Acerca de esta tarea

En el siguiente procedimiento, se quitan los switches de clúster de dos nodos y se reemplaza cada conexión al switch por una conexión directa al nodo compañero.



Acerca de los ejemplos

Los ejemplos del siguiente procedimiento muestran nodos que utilizan «e0a» y «e0b» como puertos del clúster. Sus nodos pueden usar distintos puertos de clúster según varían según el sistema.

Paso 1: Preparación para la migración

1. Cambie el nivel de privilegio a Advanced, introduzca y cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado *> aparece.

2. ONTAP 9.3 y versiones posteriores admiten la detección automática de clústeres sin switch, que está habilitado de forma predeterminada.

Puede verificar que la detección de clústeres sin switch esté habilitada mediante el comando de privilegio avanzado:

```
network options detect-switchless-cluster show
```

Muestra el ejemplo

El siguiente resultado de ejemplo muestra si la opción está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Si la opción "Activar detección de clústeres sin switch" es `false` Póngase en contacto con el soporte de NetApp.

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

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

donde h es la duración del plazo de mantenimiento en horas. El mensaje notifica al soporte técnico de esta tarea de mantenimiento para que estos puedan impedir la creación automática de casos durante la ventana de mantenimiento.

En el ejemplo siguiente, el comando suprime la creación automática de casos durante dos horas:

Muestra el ejemplo

```
cluster::*> system node autosupport invoke -node * -type all
-mmessage MAINT=2h
```

Paso 2: Configure los puertos y el cableado

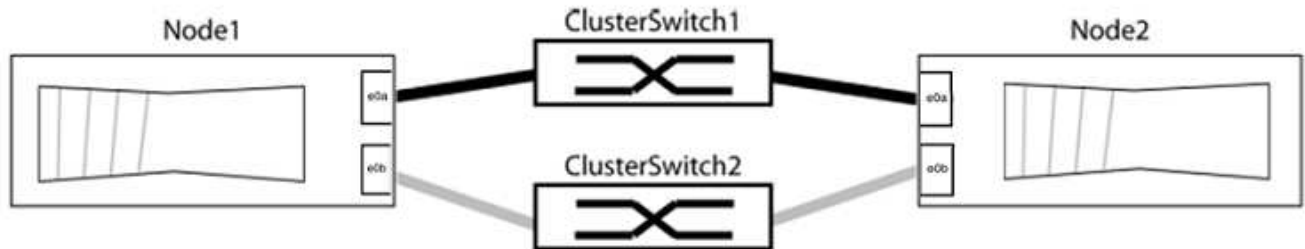
1. Organice los puertos del clúster en cada switch en grupos de modo que los puertos del clúster en group1 vayan a Cluster switch1 y los puertos del cluster en group2 vayan a cluster switch2. Estos grupos son

necesarios más adelante en el procedimiento.

2. Identificar los puertos del clúster y verificar el estado y el estado del enlace:

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

En el siguiente ejemplo, en el caso de nodos con puertos de clúster "e0a" y "e0b", un grupo se identifica como "1:e0a" y "2:e0a" y el otro grupo como "1:e0b" y "2:e0b". Sus nodos pueden usar puertos de clúster diferentes porque varían según el sistema.



Compruebe que los puertos tienen un valor de `up` Para la columna "Link" y un valor de `healthy` Para la columna "Estado de salud".

Muestra el ejemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

3. Confirmar que todas las LIF de clúster están en sus puertos raíz.

Compruebe que la columna "es-home" es true Para cada LIF del clúster:

```
network interface show -vserver Cluster -fields is-home
```

Muestra el ejemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-----  -
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Si hay LIF de clúster que no estén en sus puertos raíz, revierte estos LIF a sus puertos principales:

```
network interface revert -vserver Cluster -lif *
```

4. Deshabilite la reversión automática para las LIF del clúster:

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

5. Compruebe que todos los puertos enumerados en el paso anterior están conectados a un conmutador de red:

```
network device-discovery show -port cluster_port
```

La columna “dispositivo detectado” debe ser el nombre del conmutador de clúster al que está conectado el puerto.

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster «e0a» y «e0b» están conectados correctamente a los switches del clúster «cs1» y «cs2».

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e0a    cs1                      0/11       BES-53248
          e0b    cs2                      0/12       BES-53248
node2/cdp
          e0a    cs1                      0/9        BES-53248
          e0b    cs2                      0/9        BES-53248
4 entries were displayed.
```

6. Compruebe la conectividad del clúster:

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

7. Compruebe que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

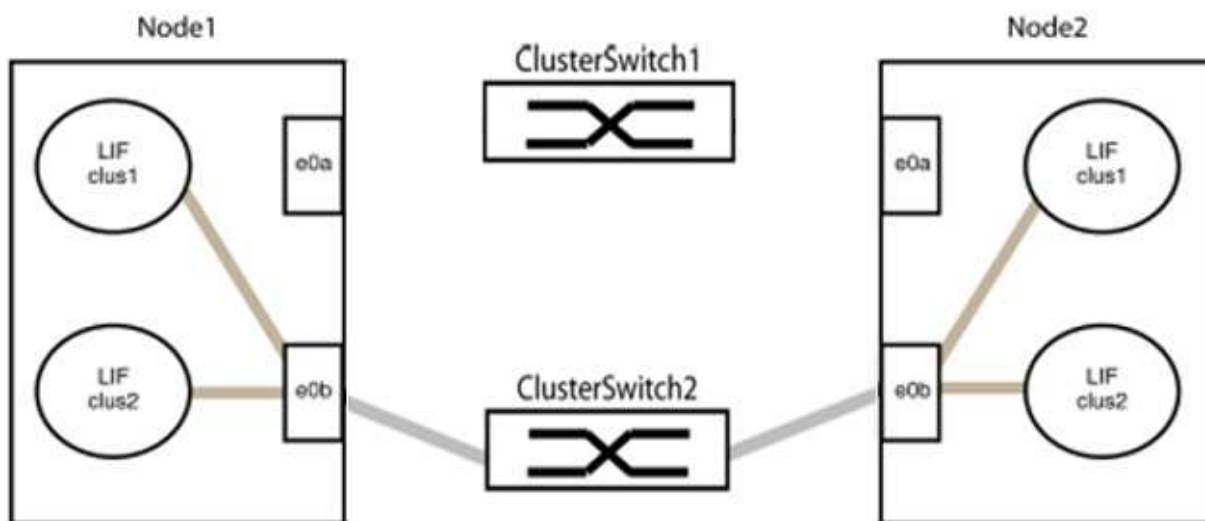
8. Configure la configuración sin switches para los puertos del grupo 1.



Para evitar posibles problemas de red, debe desconectar los puertos del grupo 1 y volver a conectarlos lo antes posible, por ejemplo, **en menos de 20 segundos**.

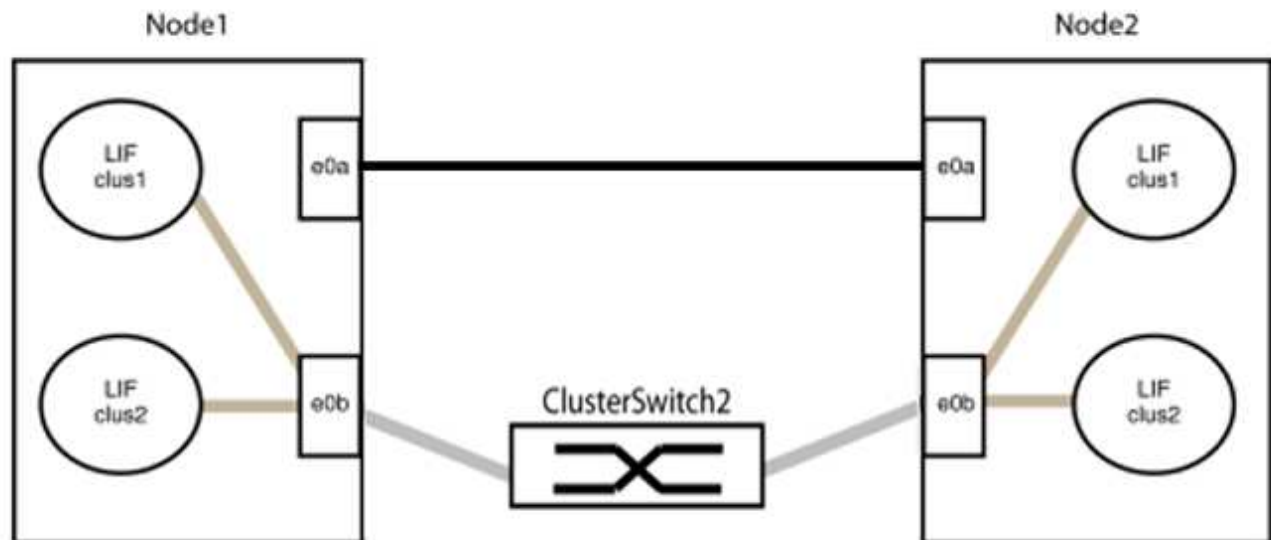
a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

En el ejemplo siguiente, los cables se desconectan del puerto "e0a" en cada nodo, y el tráfico del clúster continúa a través del switch y el puerto "e0b" en cada nodo:



b. Conecte los puertos en group1 de vuelta a espalda.

En el siguiente ejemplo, "e0a" en el nodo 1 está conectado a "e0a" en el nodo 2:



9. La opción de red de clúster sin switch desde la transición `false` para `true`. Esto puede tardar hasta 45 segundos. Confirme que la opción sin switches está establecida en `true`:

```
network options switchless-cluster show
```

En el siguiente ejemplo se muestra que el clúster sin switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

10. Compruebe que la red de clúster no se haya interrumpido:

```
cluster ping-cluster -node local
```



Antes de continuar con el siguiente paso, debe esperar al menos dos minutos para confirmar una conexión de retroceso en funcionamiento en el grupo 1.

11. Configure la configuración sin switches para los puertos del grupo 2.



Para evitar posibles problemas de red, debe desconectar los puertos del grupo 2 y volver a conectarlos lo antes posible, por ejemplo, **en menos de 20 segundos**.

- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

En el ejemplo siguiente, los cables se han desconectado del puerto "e0b" en cada nodo y el tráfico del clúster continúa por la conexión directa entre los puertos "e0a":



b. Conecte los puertos en group2 de vuelta a back.

En el ejemplo siguiente, hay conectado "e0a" en el nodo 1 a "e0a" en el nodo 2 y "e0b" en el nodo 1 está conectado a "e0b" en el nodo 2:



Paso 3: Verificar la configuración

1. Compruebe que los puertos de ambos nodos están conectados correctamente:

```
network device-discovery show -port cluster_port
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster «e0a» y «e0b» están conectados correctamente al puerto correspondiente del partner de clúster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
           e0a    node2                      e0a        AFF-A300
           e0b    node2                      e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                      e0a        AFF-A300
           e0b    node1                      e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Volver a habilitar la reversión automática para las LIF del clúster:

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

3. Compruebe que todas las LIF son Home. Esto puede tardar unos segundos.

```
network interface show -vserver Cluster -lif lif_name
```

Muestra el ejemplo

Los LIF se han revertido si la columna “es de inicio” es true, como se muestra para node1_clus2 y.. node2_clus2 en el siguiente ejemplo:

```
cluster::> network interface show -vserver Cluster -fields curr-  
port,is-home  
vserver  lif                curr-port is-home  
-----  
Cluster  node1_clus1         e0a      true  
Cluster  node1_clus2         e0b      true  
Cluster  node2_clus1         e0a      true  
Cluster  node2_clus2         e0b      true  
4 entries were displayed.
```

Si alguna LIFS de cluster no ha regresado a sus puertos de directorio raíz, revierta manualmente desde el nodo local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Compruebe el estado del clúster de los nodos desde la consola del sistema de cualquier nodo:

```
cluster show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra *epsilon* en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true        false  
node2 true    true        false  
2 entries were displayed.
```

5. Confirme la conectividad entre los puertos del clúster:

```
cluster ping-cluster local
```

6. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Para obtener más información, consulte ["Artículo de la base de conocimientos de NetApp 1010449: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#).

7. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

CN1610 de NetApp

Descripción general de la instalación y la configuración de los switches CN1610 de NetApp

El CN1610 es un switch de capa 2 gestionado con alto ancho de banda que proporciona puertos SFP+ (Small Form-factor Pluggable Plus) de 16 10 gigabits.

El switch incluye suministros de alimentación redundantes y soportes de ventiladores que admiten el intercambio en caliente para alta disponibilidad. Este switch 1U se puede instalar en un armario estándar de sistemas 42U de 19 pulgadas de NetApp o en armario de terceros.

El conmutador admite la administración local a través del puerto de consola o la administración remota utilizando Telnet o SSH a través de una conexión de red. El CN1610 incluye un puerto de gestión RJ45 Ethernet de 1 Gigabit dedicado para la gestión de switches fuera de banda. Puede gestionar el switch introduciendo comandos en la interfaz de línea de comandos (CLI) o mediante un sistema de gestión de red basado en SNMP (NMS).

Instalar y configurar el flujo de trabajo de los switches CN1610 de NetApp

Para instalar y configurar un switch NetApp CN1610 en sistemas que ejecutan ONTAP, siga estos pasos:

1. ["Instale el hardware"](#)
2. ["Instale el software FASTPATH"](#)
3. ["Instalar el archivo de configuración de referencia"](#)

Si el switch funciona con ONTAP 8.3.1 o posterior, siga las instrucciones de ["Instale FASTPATH y RVC en switches que ejecutan ONTAP 8.3.1 y versiones posteriores."](#)

4. ["Configurar el switch"](#)

Requisitos de documentación para los switches CN1610 de NetApp

Para la instalación y mantenimiento del switch CN1610 de NetApp, asegúrese de revisar toda la documentación recomendada.

Título del documento	Descripción
"Guía de instalación de 1G"	Descripción general de las características de hardware y software del switch CN1601 y del proceso de instalación.
"Guía de instalación de 10G"	Una descripción general de las características de hardware y software del switch CN1610 y describe las características para instalar el switch y acceder a la CLI.

Título del documento	Descripción
"Guía de instalación y configuración de switches CN1601 y CN1610"	Muestra cómo configurar el hardware y el software de switch para su entorno de clúster.
Guía del administrador del switch CN1601	<p>Proporciona ejemplos de cómo utilizar el switch CN1601 en una red típica.</p> <ul style="list-style-type: none"> • "Guía del administrador" • "Guía del administrador, Versión 1.1.x.x" • "Guía del administrador, Versión 1.2.x.x"
Referencia de comandos de CLI del switch de red CN1610	<p>Proporciona información detallada acerca de los comandos de la interfaz de línea de comandos (CLI) que utiliza para configurar el software CN1601.</p> <ul style="list-style-type: none"> • "Referencia de comandos" • "Referencia de comandos, Versión 1.1.x.x" • "Referencia de comandos, Versión 1.2.x.x"

Instalar y configurar

Instale el hardware del switch CN1610 de NetApp

Para instalar el hardware del switch CN1610 de NetApp, siga las instrucciones que se indican en una de las guías siguientes.

- ["Guía de instalación de 1G"](#).

Descripción general de las características de hardware y software del switch CN1601 y del proceso de instalación.

- ["Guía de instalación de 10G"](#)

Una descripción general de las características de hardware y software del switch CN1610 y describe las características para instalar el switch y acceder a la CLI.

Instale el software FASTPATH

Al instalar el software FASTPATH en los switches de NetApp, debe comenzar la actualización con el segundo switch cs2.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster que funciona completamente (sin errores en los registros y sin tarjetas de interfaz de red (NIC) del clúster defectuosas o problemas similares).

- Conexiones de puerto completamente funcionales en el switch de clúster.
- Todos los puertos del clúster configurados.
- Toda la configuración de las interfaces lógicas (LIF) del clúster (no debe haberse migrado).
- Una ruta de comunicación correcta: El ONTAP (privilegio: Avanzado) `cluster ping-cluster -node node1` el comando debe indicar que `larger than PMTU communication` se realiza correctamente en todas las rutas.
- Una versión compatible de FASTPATH y ONTAP.

Asegúrese de consultar la tabla de compatibilidad de los interruptores en la ["Switches CN1601 y CN1610 de NetApp"](#) Página para las versiones DE FASTPATH y ONTAP admitidas.

Instale FASTPATH

El siguiente procedimiento usa la sintaxis de Clustered Data ONTAP 8.2. Como resultado, los Vserver del clúster, los nombres LIF y la salida de la CLI son distintos a los de Data ONTAP 8.3.

Puede haber dependencias de comandos entre la sintaxis de comandos en las versiones RCF y FASTPATH.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los dos switches de NetApp son cs1 y cs2.
- Las dos LIF de clúster quedan clus1 y clus2.
- Los vServers son vs1 y vs2.
- La `cluster::*>` prompt indica el nombre del clúster.
- Los puertos de clúster de cada nodo se denominan e1a y e2a.

["Hardware Universe"](#) dispone de más información sobre los puertos de clúster que admiten su plataforma.

- Los enlaces Inter-Switch (ISL) compatibles son los puertos 0/13 a 0/16.
- Las conexiones de nodos admitidas son los puertos 0/1 a 0/12.

Paso 1: Migrar el clúster

1. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x es la duración de la ventana de mantenimiento en horas.



El mensaje de AutoSupport notifica al soporte técnico de esta tarea de mantenimiento para que la creación automática de casos se suprima durante la ventana de mantenimiento.

2. Inicie sesión en el switch como admin. De forma predeterminada, no hay ninguna contraseña. En la (cs2) # introduzca el `enable` comando. De nuevo, no hay contraseña de forma predeterminada. Esto le permite acceder al modo EXEC privilegiado, que le permite configurar la interfaz de red.

Muestra el ejemplo

```
(cs2) # enable
Password (Enter)
(cs2) #
```

3. En la consola de cada nodo, migre clus2 al puerto e1a:

```
network interface migrate
```

Muestra el ejemplo

```
cluster::*> network interface migrate -vserver vs1 -lif clus2
-destnode node1 -dest-port e1a
cluster::*> network interface migrate -vserver vs2 -lif clus2
-destnode node2 -dest-port e1a
```

4. En la consola de cada nodo, compruebe que la migración tuvo lugar:

```
network interface show
```

En el ejemplo siguiente se muestra que clus2 ha migrado al puerto e1a en ambos nodos:

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
```

Vserver	Logical Interface	Status Admin/Open	Network Address/Mask	Current Node	Current Port	Is Home
vs1						
	clus1	up/up	10.10.10.1/16	node1	e1a	true
	clus2	up/up	10.10.10.2/16	node1	e1a	
false						
vs2						
	clus1	up/up	10.10.10.1/16	node2	e1a	true
	clus2	up/up	10.10.10.2/16	node2	e1a	
false						

Paso 2: Instale el software FASTPATH

1. Apague el puerto e2a del clúster en ambos nodos:

```
network port modify
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el puerto e2a que se está apagando en ambos nodos:

```
cluster::*> network port modify -node node1 -port e2a -up-admin  
false  
cluster::*> network port modify -node node2 -port e2a -up-admin  
false
```

2. Compruebe que el puerto e2a está apagado en ambos nodos:

```
network port show
```

Muestra el ejemplo

```
cluster::*> network port show -role cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper
-----	----	-----	----	-----	-----	-----	-----

node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000

3. Apague los puertos de enlace entre switches (ISL) en cs1, el switch activo de NetApp:

Muestra el ejemplo

```
(cs1) # configure  
(cs1)(config) # interface 0/13-0/16  
(cs1)(Interface 0/13-0/16) # shutdown  
(cs1)(Interface 0/13-0/16) # exit  
(cs1)(config) # exit
```

4. Realice una copia de seguridad de la imagen activa actual en cs2.

Muestra el ejemplo

```
(cs2) # show bootvar

Image Descriptions      .

  active:
  backup:

Images currently available on Flash

-----
--
  unit          active      backup      current-active      next-
active
-----
--

      1          1.1.0.3      1.1.0.1          1.1.0.3          1.1.0.3

(cs2) # copy active backup
Copying active to backup
Copy operation successful

(cs2) #
```

5. Descargue el archivo de imagen en el switch.

Copiar el archivo de imagen en la imagen activa significa que cuando se reinicia, esa imagen establece la versión DE FASTPATH en ejecución. La imagen anterior sigue estando disponible como copia de seguridad.

Muestra el ejemplo

```
(cs2) # copy tftp://10.0.0.1/NetApp_CN1610_1.1.0.5.stk active

Mode..... TFTP
Set Server IP..... 10.0.0.1
Path..... ./
Filename..... NetApp_CN1610_1.1.0.5.stk
Data Type..... Code
Destination Filename..... active

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
TFTP Code transfer starting...

File transfer operation completed successfully.
```

6. Compruebe la versión de ejecución del software FASTPATH.

```
show version
```

Muestra el ejemplo

```
(cs2) # show version

Switch: 1

System Description..... Broadcom Scorpion 56820
                        Development System - 16 TENGIG,
                        1.1.0.3, Linux 2.6.21.7
Machine Type..... Broadcom Scorpion 56820
                        Development System - 16TENGIG
Machine Model..... BCM-56820
Serial Number..... 10611100004
FRU Number.....
Part Number..... BCM56820
Maintenance Level..... A
Manufacturer..... 0xbc00
Burned In MAC Address..... 00:A0:98:4B:A9:AA
Software Version..... 1.1.0.3
Operating System..... Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Additional Packages..... FASTPATH QOS
                        FASTPATH IPv6 Management
```

7. Ver las imágenes de arranque para la configuración activa y de copia de seguridad.

```
show bootvar
```

Muestra el ejemplo

```
(cs2) # show bootvar

Image Descriptions

  active :
  backup :

  Images currently available on Flash

-----
--
  unit          active          backup      current-active      next-
active
-----
--

      1          1.1.0.3        1.1.0.3        1.1.0.3        1.1.0.5
```

8. Reinicie el conmutador.

reload

Muestra el ejemplo

```
(cs2) # reload

Are you sure you would like to reset the system? (y/n)  y

System will now restart!
```

Paso 3: Validar la instalación

1. Inicie sesión de nuevo y verifique la nueva versión del software FASTPATH.

show version

Muestra el ejemplo

```
(cs2) # show version

Switch: 1

System Description..... Broadcom Scorpion 56820
                          Development System - 16
TENGIG,
                          1.1.0.5, Linux 2.6.21.7
Machine Type.....      Broadcom Scorpion 56820
                          Development System - 16TENGIG
Machine Model.....      BCM-56820
Serial Number.....      10611100004
FRU Number.....
Part Number.....        BCM56820
Maintenance Level.....   A
Manufacturer.....        0xbc00
Burned In MAC Address..... 00:A0:98:4B:A9:AA
Software Version.....    1.1.0.5
Operating System.....    Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Additional Packages.....  FASTPATH QOS
                          FASTPATH IPv6 Management
```

2. Conecte los puertos ISL en cs1, el switch activo.

```
configure
```

Muestra el ejemplo

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (Interface 0/13-0/16) # no shutdown
(cs1) (Interface 0/13-0/16) # exit
(cs1) (config) # exit
```

3. Compruebe que los ISL estén operativos:

```
show port-channel 3/1
```

El campo Estado del enlace debe indicar Up.

Muestra el ejemplo

```
(cs2) # show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed     Active
-----
0/13     actor/long      10G Full  True
         partner/long
0/14     actor/long      10G Full  True
         partner/long
0/15     actor/long      10G Full  True
         partner/long
0/16     actor/long      10G Full  True
         partner/long
```

4. Copie el running-config en la startup-config archivo cuando esté satisfecho con las versiones de software y la configuración del switch.

Muestra el ejemplo

```
(cs2) # write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .

Configuration Saved!
```

5. Habilite el segundo puerto de clúster, e2a, en cada nodo:

```
network port modify
```

Muestra el ejemplo

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> **network port modify -node node2 -port e2a -up-admin
true**
```

6. Reversión2 que está asociado al puerto e2a:

```
network interface revert
```

Es posible que LIF se revierte automáticamente en función de su versión del software ONTAP.

Muestra el ejemplo

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

7. Compruebe que la LIF se encuentra ahora en casa (true) en ambos nodos:

```
network interface show -role cluster
```

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs1	clus1	up/up	10.10.10.1/24	node1	e1a	true
	clus2	up/up	10.10.10.2/24	node1	e2a	true
vs2	clus1	up/up	10.10.10.1/24	node2	e1a	true
	clus2	up/up	10.10.10.2/24	node2	e2a	true

8. Vea el estado de los nodos:

```
cluster show
```

Muestra el ejemplo

```
cluster::> cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

9. Repita los pasos anteriores para instalar EL software FASTPATH en el otro switch, cs1.
10. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Instale un archivo de configuración de referencia en un conmutador CN1610

Siga este procedimiento para instalar un archivo de configuración de referencia (RCF).

Antes de instalar un RCF, primero debe migrar las LIF del clúster fuera del switch cs2. Una vez instalado y validado el RCF, es posible volver a migrar los LIF.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster que funciona completamente (sin errores en los registros y sin tarjetas de interfaz de red (NIC) del clúster defectuosas o problemas similares).
- Conexiones de puerto completamente funcionales en el switch de clúster.
- Todos los puertos del clúster configurados.
- Todas las interfaces lógicas (LIF) del clúster están configuradas.
- Una ruta de comunicación correcta: El ONTAP (privilegio: Avanzado) `cluster ping-cluster -node node1` el comando debe indicar que `larger than PMTU communication` se realiza correctamente en todas las rutas.
- Una versión compatible de RCF y ONTAP.

Asegúrese de consultar la tabla de compatibilidad de los interruptores en la ["Switches CN1601 y CN1610 de NetApp"](#) Para las versiones RCF y ONTAP admitidas.

Instale el RCF

El siguiente procedimiento usa la sintaxis de Clustered Data ONTAP 8.2. Como resultado, los Vserver del clúster, los nombres LIF y la salida de la CLI son distintos a los de Data ONTAP 8.3.

Puede haber dependencias de comandos entre la sintaxis de comandos en las versiones RCF y FASTPATH.



En la versión 1.2 de RCF, la compatibilidad con Telnet se ha desactivado explícitamente debido a problemas de seguridad. Para evitar problemas de conectividad durante la instalación de RCF 1.2, compruebe que Secure Shell (SSH) está habilitado. La ["Guía para administradores de switches NetApp CN1610"](#) Tiene más información acerca de SSH.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los dos switches de NetApp son cs1 y cs2.
- Las dos LIF de clúster quedan clus1 y clusa2.
- Los vServers son vs1 y vs2.
- La `cluster: *>` prompt indica el nombre del clúster.
- Los puertos de clúster de cada nodo se denominan e1a y e2a.

["Hardware Universe"](#) dispone de más información sobre los puertos de clúster que admiten su plataforma.

- Los enlaces Inter-Switch (ISL) compatibles son los puertos 0/13 a 0/16.
- Las conexiones de nodos admitidas son los puertos 0/1 a 0/12.
- Una versión compatible de FASTPATH, RCF y ONTAP.

Asegúrese de consultar la tabla de compatibilidad de los interruptores en la ["Switches CN1601 y CN1610 de NetApp"](#) Página para las versiones DE FASTPATH, RCF y ONTAP compatibles.

Paso 1: Migrar el clúster

1. Guarde la información de configuración actual del switch:

```
write memory
```

Muestra el ejemplo

En el ejemplo siguiente se muestra la configuración actual del switch que se está guardando en la configuración de inicio (`startup-config`) archivo en el conmutador cs2:

```
(cs2) # write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

2. En la consola de cada nodo, migre clus2 al puerto e1a:

```
network interface migrate
```

Muestra el ejemplo

```
cluster::*> network interface migrate -vserver vs1 -lif clus2
-source-node node1 -destnode node1 -dest-port e1a

cluster::*> network interface migrate -vserver vs2 -lif clus2
-source-node node2 -destnode node2 -dest-port e1a
```

3. En la consola de cada nodo, compruebe que se ha producido la migración:

```
network interface show -role cluster
```

Muestra el ejemplo

En el ejemplo siguiente se muestra que clus2 ha migrado al puerto e1a en ambos nodos:

```
cluster::*> network port show -role cluster
      clus1      up/up      10.10.10.1/16      node2      e1a      true
      clus2      up/up      10.10.10.2/16      node2      e1a
false
```

4. Apague el puerto e2a en ambos nodos:

```
network port modify
```

Muestra el ejemplo

En el siguiente ejemplo se muestra el puerto e2a que se está apagando en ambos nodos:

```
cluster::*> network port modify -node node1 -port e2a -up-admin
false
cluster::*> network port modify -node node2 -port e2a -up-admin
false
```

5. Compruebe que el puerto e2a está apagado en ambos nodos:

```
network port show
```

Muestra el ejemplo

```
cluster::*> network port show -role cluster
```

		(Mbps)			Auto-Negot	Duplex	Speed
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper

node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000

6. Apague los puertos ISL en cs1, el switch activo de NetApp.

Muestra el ejemplo

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (interface 0/13-0/16) # shutdown
(cs1) (interface 0/13-0/16) # exit
(cs1) (config) # exit
```

Paso 2: Instalar RCF

1. Copie el RCF en el conmutador.



Debe configurar el `.scr` extensión como parte del nombre de archivo antes de llamar al script. Esta extensión es la extensión para el sistema operativo FASTPATH.

El conmutador validará automáticamente la secuencia de comandos cuando se descargue en el conmutador y la salida pasará a la consola.

Muestra el ejemplo

```
(cs2) # copy tftp://10.10.0.1/CN1610_CS_RCF_v1.1.txt nvram:script
CN1610_CS_RCF_v1.1.scr

[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```

2. Compruebe que la secuencia de comandos se ha descargado y guardado con el nombre de archivo que le ha proporcionado.

Muestra el ejemplo

```
(cs2) # script list
Configuration Script Name          Size(Bytes)
-----
running-config.scr                6960
CN1610_CS_RCF_v1.1.scr            2199

2 configuration script(s) found.
6038 Kbytes free.
```

3. Valide el script.



El script se valida durante la descarga para verificar que cada línea es una línea de comandos del switch válida.

Muestra el ejemplo

```
(cs2) # script validate CN1610_CS_RCF_v1.1.scr
[the script is now displayed line by line]
Configuration script 'CN1610_CS_RCF_v1.1.scr' validated.
```

4. Aplique la secuencia de comandos al conmutador.

Muestra el ejemplo

```
(cs2) #script apply CN1610_CS_RCF_v1.1.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.1.scr' applied.
```

5. Compruebe que los cambios se han implementado en el conmutador.

```
(cs2) # show running-config
```

En el ejemplo se muestra la `running-config` archivo en el conmutador. Debe comparar el archivo con el RCF para comprobar que los parámetros que ha establecido son los esperados.

6. Guarde los cambios.
7. Ajuste la `running-config` el archivo será el estándar.

Muestra el ejemplo

```
(cs2) # write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.
```

8. Reinicie el switch y compruebe que `running-config` el archivo es correcto.

Cuando finalice el reinicio, debe iniciar sesión, vea el `running-config` Archivo y, a continuación, busque la descripción en la interfaz 3/64, que es la etiqueta de versión para el RCF.

Muestra el ejemplo

```
(cs2) # reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

9. Conecte los puertos ISL en cs1, el switch activo.

Muestra el ejemplo

```
(cs1) # configure
(cs1) (config)# interface 0/13-0/16
(cs1) (Interface 0/13-0/16)# no shutdown
(cs1) (Interface 0/13-0/16)# exit
(cs1) (config)# exit
```

10. Compruebe que los ISL estén operativos:

```
show port-channel 3/1
```

El campo Estado del enlace debe indicar Up.

Muestra el ejemplo

```
(cs2) # show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----
0/13      actor/long      10G Full   True
          partner/long
0/14      actor/long      10G Full   True
          partner/long
0/15      actor/long      10G Full   True
          partner/long
0/16      actor/long      10G Full   True
          partner/long
```

11. Conecte el puerto del clúster e2a en ambos nodos:

```
network port modify
```

Muestra el ejemplo

En el ejemplo siguiente, se muestra el puerto e2a en los nodos 1 y 2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

Paso 3: Validar la instalación

1. Compruebe que el puerto e2a esté activo en ambos nodos:

```
network port show -role cluster
```

Muestra el ejemplo

```
cluster::*> network port show -role cluster
```

Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
node1	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	up	9000	true/true	full/full	auto/10000
node2	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	up	9000	true/true	full/full	auto/10000

2. En ambos nodos, revierte la clus2 asociada con el puerto e2a:

```
network interface revert
```

Es posible que el LIF se revierte automáticamente en función de su versión de ONTAP.

Muestra el ejemplo

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```

3. Compruebe que la LIF se encuentra ahora en casa (true) en ambos nodos:

```
network interface show -role cluster
```

Muestra el ejemplo

```
cluster::*> network interface show -role cluster
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs1	clus1	up/up	10.10.10.1/24	node1	e1a	true
	clus2	up/up	10.10.10.2/24	node1	e2a	true
vs2	clus1	up/up	10.10.10.1/24	node2	e1a	true
	clus2	up/up	10.10.10.2/24	node2	e2a	true

4. Vea el estado de los miembros del nodo:

```
cluster show
```

Muestra el ejemplo

```
cluster::> cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

5. Copie el running-config en la startup-config archivo cuando esté satisfecho con las versiones de software y la configuración del switch.

Muestra el ejemplo

```
(cs2) # write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

6. Repita los pasos anteriores para instalar el RCF en el otro interruptor, cs1.

Instale el software FASTPATH y los RCF para ONTAP 8.3.1 y posterior

Siga este procedimiento para instalar el software FASTPATH y los RCF para ONTAP 8.3.1 y versiones posteriores.

Los pasos de instalación son los mismos para los switches de administración CN1601 de NetApp y los switches de clúster CN1610 que ejecutan ONTAP 8.3.1 o posterior. Sin embargo, los dos modelos requieren software y RVC diferentes.

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.

- Un clúster que funciona completamente (sin errores en los registros y sin tarjetas de interfaz de red (NIC) del clúster defectuosas o problemas similares).
- Conexiones de puerto completamente funcionales en el switch de clúster.
- Todos los puertos del clúster configurados.
- Toda la configuración de las interfaces lógicas (LIF) del clúster (no debe haberse migrado).
- Una ruta de comunicación correcta: El ONTAP (privilegio: Avanzado) `cluster ping-cluster -node node1` el comando debe indicar que `larger than PMTU communication` se realiza correctamente en todas las rutas.
- Una versión compatible de FASTPATH, RCF y ONTAP.

Asegúrese de consultar la tabla de compatibilidad de los interruptores en la "[Switches CN1601 y CN1610 de NetApp](#)" Página para las versiones DE FASTPATH, RCF y ONTAP compatibles.

Instale el software FASTPATH

El siguiente procedimiento usa la sintaxis de Clustered Data ONTAP 8.2. Como resultado, los Vserver del clúster, los nombres LIF y la salida de la CLI son distintos a los de Data ONTAP 8.3.

Puede haber dependencias de comandos entre la sintaxis de comandos en las versiones RCF y FASTPATH.



En la versión 1.2 de RCF, la compatibilidad con Telnet se ha desactivado explícitamente debido a problemas de seguridad. Para evitar problemas de conectividad durante la instalación de RCF 1.2, compruebe que Secure Shell (SSH) está habilitado. La "[Guía para administradores de switches NetApp CN1610](#)" Tiene más información acerca de SSH.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los dos nombres de los switches de NetApp son cs1 y cs2.
- Los nombres de la interfaz lógica del clúster (LIF) son 1_clus1 y 1_clus2 para los nodos 1, y 2_clus1 y 2_clus2 para los nodos 2. (Puede tener hasta 24 nodos en un clúster).
- El nombre de la máquina virtual de almacenamiento (SVM) es Cluster.
- La `cluster1::*>` prompt indica el nombre del clúster.
- Los puertos del clúster de cada nodo se denominan e0a y e0b.

"[Hardware Universe](#)" dispone de más información sobre los puertos de clúster que admiten su plataforma.

- Los enlaces Inter-Switch (ISL) compatibles son los puertos 0/13 a 0/16.
- Las conexiones de nodos admitidas son los puertos 0/1 a 0/12.

Paso 1: Migrar el clúster

1. Muestra información sobre los puertos de red del clúster:

```
network port show -ipspace cluster
```

Muestra el ejemplo

En el ejemplo siguiente se muestra el tipo de resultado del comando:

```
cluster1::> network port show -ipspace cluster
```

					Speed
(Mbps)					
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					
-----	-----	-----	-----	-----	-----
node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					
4 entries were displayed.					

2. Muestra información acerca de las LIF en el clúster:

```
network interface show -role cluster
```

Muestra el ejemplo

En el siguiente ejemplo se muestran las interfaces lógicas en el clúster. En este ejemplo, la `-role` El parámetro muestra información acerca de las LIF asociadas con los puertos del clúster:

```
cluster1::> network interface show -role cluster
(network interface show)

      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
Cluster
e0a      node1_clus1  up/up      10.254.66.82/16    node1
true
e0b      node1_clus2  up/up      10.254.206.128/16  node1
true
e0a      node2_clus1  up/up      10.254.48.152/16   node2
true
e0b      node2_clus2  up/up      10.254.42.74/16    node2
true
4 entries were displayed.
```

3. En cada nodo correspondiente, utilizando una LIF de gestión de nodos, migre 1_clus2 a e0a en el nodo 1 y 2_clus2 a e0a en el nodo 2:

```
network interface migrate
```

Debe introducir los comandos en las consolas de la controladora que sean las respectivas LIF de clúster.

Muestra el ejemplo

```
cluster1::> network interface migrate -vserver Cluster -lif
node1_clus2 -destination-node node1 -destination-port e0a
cluster1::> network interface migrate -vserver Cluster -lif
node2_clus2 -destination-node node2 -destination-port e0a
```



Para este comando, el nombre del clúster distingue mayúsculas de minúsculas y se debe ejecutar el comando en cada nodo. No es posible ejecutar este comando en la LIF de clúster general.

4. Compruebe que la migración se ha realizado mediante el `network interface show` comando en un nodo.

Muestra el ejemplo

En el siguiente ejemplo, se muestra que clus2 ha migrado al puerto e0a en los nodos 1 y 2:

```
cluster1::> **network interface show -role cluster**
          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
          node1_clus1  up/up      10.254.66.82/16   node1
e0a       true
          node1_clus2  up/up      10.254.206.128/16 node1
e0a       false
          node2_clus1  up/up      10.254.48.152/16  node2
e0a       true
          node2_clus2  up/up      10.254.42.74/16  node2
e0a       false
4 entries were displayed.
```

5. Cambie el nivel de privilegio a avanzado, introduciendo y cuando se le solicite continuar:

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

6. Apague el puerto e0b del clúster en ambos nodos:

```
network port modify -node node_name -port port_name -up-admin false
```

Debe introducir los comandos en las consolas de la controladora que sean las respectivas LIF de clúster.

Muestra el ejemplo

En el siguiente ejemplo, se muestran los comandos para apagar el puerto e0b en todos los nodos:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin
false
cluster1::*> network port modify -node node2 -port e0b -up-admin
false
```

7. Compruebe que el puerto e0b está apagado en ambos nodos:

network port show

Muestra el ejemplo

```
cluster1::*> network port show -role cluster
```

					Speed
(Mbps)					
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					
-----	-----	-----	-----	-----	-----

node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	down	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	down	9000
auto/10000					
4 entries were displayed.					

8. Apague los puertos de enlace entre switches (ISL) en cs1.

Muestra el ejemplo

```
(cs1) #configure
(cs1) (Config)#interface 0/13-0/16
(cs1) (Interface 0/13-0/16)#shutdown
(cs1) (Interface 0/13-0/16)#exit
(cs1) (Config)#exit
```

9. Realice una copia de seguridad de la imagen activa actual en cs2.

Muestra el ejemplo

```
(cs2) # show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active

1	1.1.0.5	1.1.0.3	1.1.0.5	1.1.0.5

```
(cs2) # copy active backup
```

Copying active to backup

Copy operation successful

Paso 2: Instale EL software FASTPATH y RCF

1. Compruebe la versión de ejecución del software FASTPATH.

Muestra el ejemplo

```
(cs2) # show version

Switch: 1

System Description..... NetApp CN1610,
1.1.0.5, Linux
                               2.6.21.7
Machine Type..... NetApp CN1610
Machine Model..... CN1610
Serial Number..... 20211200106
Burned In MAC Address..... 00:A0:98:21:83:69
Software Version..... 1.1.0.5
Operating System..... Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Part Number..... 111-00893

--More-- or (q)uit

Additional Packages..... FASTPATH QOS
                               FASTPATH IPv6
Management
```

2. Descargue el archivo de imagen en el switch.

Copiar el archivo de imagen en la imagen activa significa que cuando se reinicia, esa imagen establece la versión DE FASTPATH en ejecución. La imagen anterior sigue estando disponible como copia de seguridad.

Muestra el ejemplo

```
(cs2) #copy
sftp://root@10.22.201.50//tftpboot/NetApp_CN1610_1.2.0.7.stk active
Remote Password:*****

Mode..... SFTP
Set Server IP..... 10.22.201.50
Path..... /tftpboot/
Filename.....
NetApp_CN1610_1.2.0.7.stk
Data Type..... Code
Destination Filename..... active

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
SFTP Code transfer starting...

File transfer operation completed successfully.
```

3. Confirme las versiones actuales y las siguientes de las imágenes de arranque activas:

```
show bootvar
```

Muestra el ejemplo

```
(cs2) #show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
```

unit	active	backup	current-active	next-active
1	1.1.0.8	1.1.0.8	1.1.0.8	1.2.0.7

4. Instale el RCF compatible para la nueva versión de imagen en el conmutador.

Si la versión de RCF ya es correcta, coloque los puertos ISL.

Muestra el ejemplo

```
(cs2) #copy tftp://10.22.201.50//CN1610_CS_RCF_v1.2.txt nvram:script
CN1610_CS_RCF_v1.2.scr

Mode..... TFTP
Set Server IP..... 10.22.201.50
Path..... /
Filename.....
CN1610_CS_RCF_v1.2.txt
Data Type..... Config Script
Destination Filename.....
CN1610_CS_RCF_v1.2.scr

File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

Validating configuration script...
[the script is now displayed line by line]

Configuration script validated.
File transfer operation completed successfully.
```



La `.scr` la extensión se debe establecer como parte del nombre de archivo antes de llamar al script. Esta extensión es para el sistema operativo FASTPATH.

El switch valida el script automáticamente a medida que se descarga en el switch. La salida va a la consola.

5. Compruebe que la secuencia de comandos se ha descargado y guardado en el nombre de archivo que le ha proporcionado.

Muestra el ejemplo

```
(cs2) #script list

Configuration Script Name          Size(Bytes)
-----
CN1610_CS_RCF_v1.2.scr            2191

1 configuration script(s) found.
2541 Kbytes free.
```

6. Aplique la secuencia de comandos al conmutador.

Muestra el ejemplo

```
(cs2) #script apply CN1610_CS_RCF_v1.2.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.2.scr' applied.
```

7. Compruebe que los cambios se han aplicado al interruptor y, a continuación, guárdelos:

```
show running-config
```

Muestra el ejemplo

```
(cs2) #show running-config
```

8. Guarde la configuración en ejecución para que se convierta en la configuración de inicio al reiniciar el conmutador.

Muestra el ejemplo

```
(cs2) #write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

9. Reinicie el conmutador.

Muestra el ejemplo

```
(cs2) #reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

Paso 3: Validar la instalación

1. Inicie sesión de nuevo y, a continuación, compruebe que el switch utiliza la nueva versión del software FASTPATH.

Muestra el ejemplo

```
(cs2) #show version

Switch: 1

System Description..... NetApp CN1610,
1.2.0.7,Linux
                               3.8.13-4ce360e8
Machine Type..... NetApp CN1610
Machine Model..... CN1610
Serial Number..... 20211200106
Burned In MAC Address..... 00:A0:98:21:83:69
Software Version..... 1.2.0.7
Operating System..... Linux 3.8.13-
4ce360e8
Network Processing Device..... BCM56820_B0
Part Number..... 111-00893
CPLD version..... 0x5

Additional Packages..... FASTPATH QOS
                        FASTPATH IPv6
Management
```

Una vez completado el reinicio, debe iniciar sesión para verificar la versión de la imagen, ver la configuración en ejecución y buscar la descripción en la interfaz 3/64, que es la etiqueta de versión del RCF.

2. Conecte los puertos ISL en cs1, el switch activo.

Muestra el ejemplo

```
(cs1) #configure
(cs1) (Config) #interface 0/13-0/16
(cs1) (Interface 0/13-0/16) #no shutdown
(cs1) (Interface 0/13-0/16) #exit
(cs1) (Config) #exit
```

3. Compruebe que los ISL estén operativos:

```
show port-channel 3/1
```

El campo Estado del enlace debe indicar Up.

Muestra el ejemplo

```
(cs1) #show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----
0/13      actor/long      10G Full   True
          partner/long
0/14      actor/long      10G Full   True
          partner/long
0/15      actor/long      10G Full   False
          partner/long
0/16      actor/long      10G Full   True
          partner/long
```

4. Coloque el puerto e0b en el clúster en todos los nodos:

```
network port modify
```

Debe introducir los comandos en las consolas de la controladora que sean las respectivas LIF de clúster.

Muestra el ejemplo

En el siguiente ejemplo, se muestra la puesta en funcionamiento del puerto e0b en el nodo 1 y el nodo 2:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin
true
cluster1::*> network port modify -node node2 -port e0b -up-admin
true
```

5. Verifique que el puerto e0b esté activo en todos los nodos:

```
network port show -ipSPACE cluster
```

Muestra el ejemplo

```
cluster1::*> network port show -ipspace cluster
```

					Speed
(Mbps)					
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					
-----	-----	-----	-----	-----	-----
node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					

4 entries were displayed.

6. Compruebe que la LIF se encuentra ahora en casa (true) en ambos nodos:

```
network interface show -role cluster
```

Muestra el ejemplo

```
cluster1::*> network interface show -role cluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e0a	node1_clus1	up/up	169.254.66.82/16	node1
e0b	true			
e0a	node1_clus2	up/up	169.254.206.128/16	node1
e0b	true			
e0a	node2_clus1	up/up	169.254.48.152/16	node2
e0b	true			
e0a	node2_clus2	up/up	169.254.42.74/16	node2
e0b	true			
4 entries were displayed.				

7. Muestra el estado de los miembros del nodo:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon

node1	true	true	false
node2	true	true	false
2 entries were displayed.			

8. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

9. Repita los pasos anteriores para instalar EL software FASTPATH y RCF en el otro switch, cs1.

Configurar el hardware del switch CN1610 de NetApp

Para configurar el hardware y el software del switch para el entorno de clúster, consulte

la ["Guía de instalación y configuración de switches CN1601 y CN1610"](#).

Migrar switches

Migrar de un entorno de clúster sin switches a un entorno de clúster con switches CN1610 de NetApp

Si ya dispone de un entorno de clúster sin switches de dos nodos, puede migrar a un entorno de clúster con switches de dos nodos mediante switches de red de clústeres CN1610, los cuales le permiten escalar más allá de dos nodos.

Revise los requisitos

Lo que necesitará

En el caso de una configuración sin switch de dos nodos, asegúrese de que:

- La configuración sin switch de dos nodos está correctamente configurada y funciona.
- Los nodos ejecutan ONTAP 8.2 o una versión posterior.
- Todos los puertos del clúster están en la `up` estado.
- Todas las interfaces lógicas (LIF) del clúster están en la `up` estado y en sus puertos de origen.

Para la configuración del switch de clúster CN1610:

- La infraestructura de switches de clúster CN1610 es completamente funcional en ambos switches.
- Ambos switches tienen conectividad de red de gestión.
- Hay acceso de la consola a los switches de clúster.
- Las conexiones de switch a nodo CN1610 y de switch a switch utilizan cables de fibra óptica o twinax.

La ["Hardware Universe"](#) contiene más información sobre el cableado.

- Los cables de enlace entre switches (ISL) se conectan a los puertos 13 a 16 en los dos switches CN1610.
- Se ha completado la personalización inicial de los dos switches CN1610.

Cualquier personalización anterior del sitio, como SMTP, SNMP y SSH, se debe copiar a los nuevos switches.

Información relacionada

- ["Hardware Universe"](#)
- ["Página de descripción de NetApp CN1601 y CN1610"](#)
- ["Guía de instalación y configuración de switches CN1601 y CN1610"](#)
- ["Artículo de la base de conocimientos de NetApp 1010449: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#)

Migrar los switches

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la siguiente nomenclatura de nodo y conmutador de cluster:

- Los nombres de los switches CN1610 son `cs1` y `cs2`.

- Los nombres de las LIF se incluyen clus1 y clus2.
- Los nombres de los nodos son 1 y 2.
- La `cluster::*>` prompt indica el nombre del clúster.
- Los puertos de clúster que se utilizan en este procedimiento son e1a y e2a.

La "[Hardware Universe](#)" contiene la información más reciente acerca de los puertos del clúster reales para las plataformas.

Paso 1: Preparación para la migración

1. Cambie el nivel de privilegio a Advanced, introduzca `y` cuando se le solicite continuar:

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

2. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

x es la duración de la ventana de mantenimiento en horas.



El mensaje de AutoSupport notifica al soporte técnico de esta tarea de mantenimiento para que la creación automática de casos se suprima durante la ventana de mantenimiento.

Muestra el ejemplo

El siguiente comando suprime la creación automática de casos durante dos horas:

```
cluster::*> system node autosupport invoke -node * -type all
-mmessage MAINT=2h
```

Paso 2: Configurar puertos

1. Deshabilite todos los puertos orientados al nodo (no los puertos ISL) en los nuevos switches de clúster cs1 y cs2.

No debe deshabilitar los puertos ISL.

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos 1 a 12 que están orientados al nodo están deshabilitados en el switch cs1:

```
(cs1)> enable
(cs1)# configure
(cs1)(Config)# interface 0/1-0/12
(cs1)(Interface 0/1-0/12)# shutdown
(cs1)(Interface 0/1-0/12)# exit
(cs1)(Config)# exit
```

En el ejemplo siguiente se muestra que los puertos 1 a 12 que están orientados al nodo están deshabilitados en el switch cs2:

```
(c2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

2. Compruebe que el ISL y los puertos físicos del ISL se encuentran entre los dos switches del clúster CN1610 cs1 y cs2 up:

```
show port-channel
```

Muestra el ejemplo

El siguiente ejemplo muestra que los puertos ISL son up en el interruptor cs1:

```
(cs1)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr Ports	Device/ Timeout	Port Speed	Port Active
-----	-----	-----	-----
0/13	actor/long partner/long	10G Full	True
0/14	actor/long partner/long	10G Full	True
0/15	actor/long partner/long	10G Full	True
0/16	actor/long partner/long	10G Full	True

El siguiente ejemplo muestra que los puertos ISL son up en el interruptor cs2:

```
(cs2)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr	Device/ Ports	Port Timeout	Port Speed	Port Active
-----	-----	-----	-----	-----
0/13	actor/long partner/long	10G Full	True	
0/14	actor/long partner/long	10G Full	True	
0/15	actor/long partner/long	10G Full	True	
0/16	actor/long partner/long	10G Full	True	

3. Mostrar la lista de dispositivos vecinos:

```
show isdp neighbors
```

Este comando proporciona información sobre los dispositivos conectados al sistema.

Muestra el ejemplo

En el siguiente ejemplo se enumeran los dispositivos vecinos del conmutador cs1:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID          Intf          Holdtime  Capability  Platform
Port ID
-----
cs2                0/13          11        S           CN1610
0/13
cs2                0/14          11        S           CN1610
0/14
cs2                0/15          11        S           CN1610
0/15
cs2                0/16          11        S           CN1610
0/16
```

En el siguiente ejemplo se enumeran los dispositivos vecinos en el conmutador cs2:

```
(cs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID          Intf          Holdtime  Capability  Platform
Port ID
-----
cs1                0/13          11        S           CN1610
0/13
cs1                0/14          11        S           CN1610
0/14
cs1                0/15          11        S           CN1610
0/15
cs1                0/16          11        S           CN1610
0/16
```

4. Mostrar la lista de puertos del clúster:

```
network port show
```

Muestra el ejemplo

En el siguiente ejemplo se muestran los puertos de clúster disponibles:

```
cluster::*> network port show -ipspace Cluster
```

```
Node: node1
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0c	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0d	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

```
Node: node2
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0c	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0d	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

```
12 entries were displayed.
```


5. Compruebe que cada puerto del clúster está conectado al puerto correspondiente en el nodo del clúster asociado:

```
run * cdpd show-neighbors
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster e1a y e2a están conectados al mismo puerto en su nodo asociado de clúster:

```
cluster::*> run * cdpd show-neighbors
2 entries were acted on.
```

Node: node1

Local Remote	Remote	Remote	Remote	Hold
Port Device	Interface	Platform	Time	
Capability				
e1a	node2	e1a	FAS3270	137
H				
e2a	node2	e2a	FAS3270	137
H				

Node: node2

Local Remote	Remote	Remote	Remote	Hold
Port Device	Interface	Platform	Time	
Capability				
e1a	node1	e1a	FAS3270	161
H				
e2a	node1	e2a	FAS3270	161
H				

6. Compruebe que todas las LIF del clúster son up y operativo:

```
network interface show -vserver Cluster
```

Cada LIF del clúster debería mostrar true En la columna «is Home».

Muestra el ejemplo

```
cluster::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
node1					
true	clus1	up/up	10.10.10.1/16	node1	e1a
true	clus2	up/up	10.10.10.2/16	node1	e2a
node2					
true	clus1	up/up	10.10.11.1/16	node2	e1a
true	clus2	up/up	10.10.11.2/16	node2	e2a

4 entries were displayed.



Los siguientes comandos de modificación y migración de los pasos 10 a 13 se deben realizar desde el nodo local.

7. Compruebe que todos los puertos del clúster lo sean up:

```
network port show -ipspace Cluster
```

Muestra el ejemplo

```
cluster::*> network port show -ipspace Cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							

node1							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

8. Ajuste la `-auto-revert` parámetro a. `false` En las LIF de cluster `clus1` y `clus2` en ambos nodos:

```
network interface modify
```

Muestra el ejemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```



Para las versiones 8.3 y posteriores, se debe utilizar el siguiente comando: `network interface modify -vserver Cluster -lif * -auto-revert false`

9. Haga ping en los puertos del clúster para verificar la conectividad de clúster:

```
cluster ping-cluster local
```

El resultado del comando muestra la conectividad entre todos los puertos del clúster.

10. Migre clus1 al puerto e2a de la consola de cada nodo:

```
network interface migrate
```

Muestra el ejemplo

En el siguiente ejemplo, se muestra el proceso de migración de clus1 al puerto e2a en los nodos 1 y 2:

```
cluster::*> network interface migrate -vserver node1 -lif clus1  
-source-node node1 -dest-node node1 -dest-port e2a  
cluster::*> network interface migrate -vserver node2 -lif clus1  
-source-node node2 -dest-node node2 -dest-port e2a
```



Para las versiones 8.3 y posteriores, se debe utilizar el siguiente comando: `network interface migrate -vserver Cluster -lif clus1 -destination-node node1 -destination-port e2a`

11. Compruebe que la migración tuvo lugar:

```
network interface show -vserver Cluster
```

Muestra el ejemplo

En el siguiente ejemplo, se verifica que la versión 1 se migra al puerto e2a en los nodos 1 y 2:

```
cluster::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
node1					
false	clus1	up/up	10.10.10.1/16	node1	e2a
true	clus2	up/up	10.10.10.2/16	node1	e2a
node2					
false	clus1	up/up	10.10.11.1/16	node2	e2a
true	clus2	up/up	10.10.11.2/16	node2	e2a

4 entries were displayed.

12. Apague el puerto del clúster e1a en ambos nodos:

```
network port modify
```

Muestra el ejemplo

En el ejemplo siguiente, se muestra cómo apagar el puerto e1a en los nodos 1 y 2:

```
cluster::*> network port modify -node node1 -port e1a -up-admin  
false  
cluster::*> network port modify -node node2 -port e1a -up-admin  
false
```

13. Compruebe el estado del puerto:

```
network port show
```

Muestra el ejemplo

En el ejemplo siguiente se muestra que el puerto e1a es down en los nodos 1 y 2:

```
cluster::*> network port show -role cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							

node1							
	e1a	clus1	down	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	down	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

- Desconecte el cable del puerto del clúster e1a del nodo 1 y, a continuación, conecte e1a al puerto 1 del switch del clúster cs1 mediante el cableado adecuado que admiten los switches CN1610.

La "[Hardware Universe](#)" contiene más información sobre el cableado.

- Desconecte el cable del puerto del clúster e1a del nodo 2 y, a continuación, conecte e1a al puerto 2 del switch del clúster cs1 mediante el cableado adecuado compatible con los switches CN1610.
- Habilite todos los puertos orientados al nodo en el switch de clúster cs1.

Muestra el ejemplo

El siguiente ejemplo muestra que los puertos 1 a 12 están habilitados en el conmutador cs1:

```
(cs1)# configure
(cs1)(Config)# interface 0/1-0/12
(cs1)(Interface 0/1-0/12)# no shutdown
(cs1)(Interface 0/1-0/12)# exit
(cs1)(Config)# exit
```

- Habilite el primer puerto de clúster e1a en cada nodo:

```
network port modify
```

Muestra el ejemplo

En el ejemplo siguiente, se muestra cómo habilitar el puerto e1a en los nodos 1 y 2:

```
cluster::*> network port modify -node node1 -port e1a -up-admin true
cluster::*> network port modify -node node2 -port e1a -up-admin true
```

18. Compruebe que todos los puertos del clúster lo sean up:

```
network port show -ipSPACE Cluster
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que todos los puertos del clúster son up en los nodos 1 y 2:

```
cluster::*> network port show -ipSPACE Cluster
                                     Auto-Negot  Duplex      Speed
(Mbps)
Node  Port  Role      Link  MTU Admin/Oper  Admin/Oper
Admin/Oper
-----
node1
      e1a   clus1    up    9000  true/true  full/full
auto/10000
      e2a   clus2    up    9000  true/true  full/full
auto/10000
node2
      e1a   clus1    up    9000  true/true  full/full
auto/10000
      e2a   clus2    up    9000  true/true  full/full
auto/10000

4 entries were displayed.
```

19. Reversión1 (que se migró anteriormente) a e1a en ambos nodos:

```
network interface revert
```

Muestra el ejemplo

En el ejemplo siguiente, se muestra cómo revertir la versión 1 al puerto e1a en el nodo 1 y el nodo 2:

```
cluster::*> network interface revert -vserver node1 -lif clus1
cluster::*> network interface revert -vserver node2 -lif clus1
```



Para las versiones 8.3 y posteriores, se debe utilizar el siguiente comando: `network interface revert -vserver Cluster -lif <nodename_clus<N>>`

20. Compruebe que todas las LIF del clúster son up, operativo y mostrar como true En la columna "es de inicio":

```
network interface show -vserver Cluster
```

Muestra el ejemplo

El ejemplo siguiente muestra que todas las LIF son up En los nodos 1 y 2, y los resultados de la columna "es Home" son true:

```
cluster::*> network interface show -vserver Cluster
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask  Node      Port
Home
-----
node1
      clus1      up/up      10.10.10.1/16  node1      e1a
true
      clus2      up/up      10.10.10.2/16  node1      e2a
true
node2
      clus1      up/up      10.10.11.1/16  node2      e1a
true
      clus2      up/up      10.10.11.2/16  node2      e2a
true

4 entries were displayed.
```

21. Muestra información sobre el estado de los nodos en el clúster:

```
cluster show
```


Muestra el ejemplo

En el siguiente ejemplo se muestra información sobre el estado y la elegibilidad de los nodos en el clúster:

```
cluster::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true    true         false
node2                true    true         false
```

22. Migre la versión 2 al puerto e1a de la consola de cada nodo:

```
network interface migrate
```

Muestra el ejemplo

En el siguiente ejemplo, se muestra el proceso de migración de clus2 al puerto e1a en los nodos 1 y 2:

```
cluster::*> network interface migrate -vserver node1 -lif clus2
-source-node node1 -dest-node node1 -dest-port e1a
cluster::*> network interface migrate -vserver node2 -lif clus2
-source-node node2 -dest-node node2 -dest-port e1a
```



Para las versiones 8.3 y posteriores, se debe utilizar el siguiente comando: `network interface migrate -vserver Cluster -lif node1_clus2 -dest-node node1 -dest-port e1a`

23. Compruebe que la migración tuvo lugar:

```
network interface show -vserver Cluster
```

Muestra el ejemplo

En el siguiente ejemplo, se verifica que la versión 2 se migra al puerto e1a en los nodos 1 y 2:

```
cluster::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
node1					
true	clus1	up/up	10.10.10.1/16	node1	e1a
false	clus2	up/up	10.10.10.2/16	node1	e1a
node2					
true	clus1	up/up	10.10.11.1/16	node2	e1a
false	clus2	up/up	10.10.11.2/16	node2	e1a

4 entries were displayed.

24. Apague el puerto e2a del clúster en ambos nodos:

```
network port modify
```

Muestra el ejemplo

En el ejemplo siguiente, se muestra cómo apagar el puerto e2a en los nodos 1 y 2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin  
false  
cluster::*> network port modify -node node2 -port e2a -up-admin  
false
```

25. Compruebe el estado del puerto:

```
network port show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que el puerto e2a es down en los nodos 1 y 2:

```
cluster::*> network port show -role cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							

node1							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	down	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	down	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

26. Desconecte el cable del puerto del clúster e2a del nodo 1 y, a continuación, conecte e2a al puerto 1 del switch del clúster cs2 mediante el cableado adecuado que admiten los switches CN1610.
27. Desconecte el cable del puerto del clúster e2a del nodo 2 y, a continuación, conecte e2a al puerto 2 del switch del clúster cs2 mediante el cableado adecuado que admiten los switches CN1610.
28. Habilite todos los puertos orientados al nodo en el switch de clúster cs2.

Muestra el ejemplo

El siguiente ejemplo muestra que los puertos 1 a 12 están habilitados en el conmutador cs2:

```
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# no shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

29. Habilite el segundo puerto e2a de clúster en cada nodo.

Muestra el ejemplo

En el ejemplo siguiente, se muestra cómo habilitar el puerto e2a en los nodos 1 y 2:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

30. Compruebe que todos los puertos del clúster lo sean up:

```
network port show -ipspace Cluster
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que todos los puertos del clúster son up en los nodos 1 y 2:

```
cluster::*> network port show -ipspace Cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							
-----	-----	-----	----	-----	-----	-----	

node1							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

31. Revert clus2 (que se migró anteriormente) a e2a en ambos nodos:

```
network interface revert
```

Muestra el ejemplo

En el ejemplo siguiente, se muestra cómo revertir clus2 al puerto e2a en los nodos 1 y 2:

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```



Para la versión 8.3 y posteriores, los comandos son: cluster::*> network interface revert -vserver Cluster -lif node1_clus2 y. cluster::*> network interface revert -vserver Cluster -lif node2_clus2

Paso 3: Completar la configuración

1. Compruebe que se muestran todas las interfaces true En la columna "es de inicio":

```
network interface show -vserver Cluster
```

Muestra el ejemplo

El ejemplo siguiente muestra que todas las LIF son up En los nodos 1 y 2, y los resultados de la columna "es Home" son true:

```
cluster::*> network interface show -vserver Cluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

node1				
	clus1	up/up	10.10.10.1/16	node1
e1a	true			
	clus2	up/up	10.10.10.2/16	node1
e2a	true			
node2				
	clus1	up/up	10.10.11.1/16	node2
e1a	true			
	clus2	up/up	10.10.11.2/16	node2
e2a	true			

2. Haga ping en los puertos del clúster para verificar la conectividad de clúster:

```
cluster ping-cluster local
```

El resultado del comando muestra la conectividad entre todos los puertos del clúster.

3. Compruebe que ambos nodos tienen dos conexiones a cada switch:

```
show isdp neighbors
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran los resultados adecuados para ambos switches:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID          Intf          Holdtime  Capability  Platform
Port ID
-----
-----
node1              0/1            132       H           FAS3270
e1a
node2              0/2            163       H           FAS3270
e1a
cs2                0/13           11        S           CN1610
0/13
cs2                0/14           11        S           CN1610
0/14
cs2                0/15           11        S           CN1610
0/15
cs2                0/16           11        S           CN1610
0/16

(cs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID          Intf          Holdtime  Capability  Platform
Port ID
-----
-----
node1              0/1            132       H           FAS3270
e2a
node2              0/2            163       H           FAS3270
e2a
cs1                0/13           11        S           CN1610
0/13
cs1                0/14           11        S           CN1610
0/14
cs1                0/15           11        S           CN1610
0/15
cs1                0/16           11        S           CN1610
0/16
```

4. Muestra información sobre los dispositivos de la configuración:

```
network device discovery show
```

5. Deshabilite la configuración de dos nodos sin switch en ambos nodos mediante el comando Advanced Privilege:

```
network options detect-switchless modify
```

Muestra el ejemplo

En el siguiente ejemplo se muestra cómo deshabilitar las opciones de configuración sin switch:

```
cluster::*> network options detect-switchless modify -enabled false
```



Para la versión 9.2 y posteriores, omita este paso ya que la configuración se convertirá automáticamente.

6. Compruebe que la configuración está desactivada:

```
network options detect-switchless-cluster show
```

Muestra el ejemplo

La `false` el resultado del ejemplo siguiente muestra que las opciones de configuración están deshabilitadas:

```
cluster::*> network options detect-switchless-cluster show  
Enable Switchless Cluster Detection: false
```



Para la versión 9.2 o posterior, espere hasta `Enable Switchless Cluster` se establece en falso. Esto puede tardar hasta tres minutos.

7. Configure los clústeres `clus1` y `clus2` para revertir automáticamente cada nodo y confirmar.

Muestra el ejemplo

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert true
```



Para las versiones 8.3 y posteriores, se debe utilizar el siguiente comando: `network interface modify -vserver Cluster -lif * -auto-revert true` para habilitar la reversión automática en todos los nodos del clúster.

8. Compruebe el estado de los miembros del nodo en el clúster:

```
cluster show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra información sobre el estado y la elegibilidad de los nodos en el clúster:

```
cluster::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true    true         false
node2                true    true         false
```

9. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Muestra el ejemplo

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=END
```

10. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

Sustituya los interruptores

Reemplace un switch de cluster CN1610 de NetApp

Siga estos pasos para reemplazar un switch CN1610 de NetApp defectuoso en una red de clúster. Se trata de un procedimiento no disruptivo (NDU).

Lo que necesitará

Antes de realizar la sustitución del switch, debe haber las siguientes condiciones antes de realizar la sustitución del switch en el entorno actual y en el switch de sustitución del clúster y la infraestructura de red existentes:

- El clúster existente debe verificarse como completamente funcional, con al menos un switch de clúster completamente conectado.
- Todos los puertos del clúster deben ser **UP**.
- Todas las interfaces lógicas (LIF) del clúster deben estar activas y no se deben haber migrado.
- El clúster de ONTAP `ping-cluster -node node1` El comando debe indicar que la conectividad básica y la comunicación más grande que la PMTU se han realizado correctamente en todas las rutas.

Acerca de esta tarea

Debe ejecutar el comando para migrar una LIF de clúster desde el nodo donde se aloja la LIF del clúster.

Los ejemplos de este procedimiento utilizan la siguiente nomenclatura de nodo y conmutador de cluster:

- Los nombres de los dos switches de clústeres CN1610 son `cs1` y.. `cs2`.
- El nombre del interruptor CN1610 que se va a sustituir (el interruptor defectuoso) es `old_cs1`.
- El nombre del nuevo interruptor CN1610 (el interruptor de reemplazo) es `new_cs1`.
- El nombre del conmutador de socio que no se va a sustituir es `cs2`.

Pasos

1. Confirme que el archivo de configuración de inicio coincide con el archivo de configuración en ejecución. Debe guardar estos archivos localmente para usarlos durante el reemplazo.

Los comandos de configuración del siguiente ejemplo son para FASTPATH 1,2.0,7:

Muestra el ejemplo

```
(old_cs1) >enable
(old_cs1) #show running-config
(old_cs1) #show startup-config
```

2. Cree una copia del archivo de configuración en ejecución.

El comando del siguiente ejemplo es para FASTPATH 1,2.0,7:

Muestra el ejemplo

```
(old_cs1) #show running-config filename.scr  
Config script created successfully.
```



Se puede utilizar cualquier nombre de archivo excepto CN1610_CS_RCF_v1.2.scr. El nombre del archivo debe tener la extensión **.scr**.

1. Guarde el archivo de configuración en ejecución del switch en un host externo como preparación para el reemplazo.

Muestra el ejemplo

```
(old_cs1) #copy nvram:script filename.scr  
scp://<Username>@<remote_IP_address>/path_to_file/filename.scr
```

2. Comprobar que las versiones del switch y de ONTAP coinciden en la matriz de compatibilidad. Consulte ["Switches CN1601 y CN1610 de NetApp"](#) para obtener más detalles.
3. Desde la ["Página de descargas de software"](#) En el sitio de soporte de NetApp, seleccione switches de clúster de NetApp para descargar las versiones de RCF y FASTPATH adecuadas.
4. Configure un servidor Trivial File Transfer Protocol (TFTP) con la configuración FASTPATH, RCF y guardada **.scr** archivo para utilizar con el nuevo conmutador.
5. Conecte el puerto serie (el conector RJ-45 etiquetado como "IOIOI" en el lado derecho del switch) a un host disponible con emulación de terminal.
6. En el host, establezca los ajustes de conexión del terminal serie:
 - a. 9600 baudios
 - b. 8 bits de datos
 - c. 1 bit de parada
 - d. paridad: none
 - e. control de flujo: ninguno
7. Conecte el puerto de administración (el puerto de llave RJ-45 en el lado izquierdo del switch) a la misma red en la que se encuentra el servidor TFTP.
8. Prepárese para conectarse a la red con el servidor TFTP.

Si utiliza el protocolo de configuración dinámica de host (DHCP), no es necesario configurar una dirección IP para el switch en este momento. El puerto de servicio está configurado para usar DHCP de forma predeterminada. El puerto de gestión de red está configurado como ninguno para la configuración del protocolo IPv4 y IPv6. Si el puerto de llave inglesa está conectado a una red que tiene un servidor DHCP, los ajustes del servidor se configuran automáticamente.

Para configurar una dirección IP estática, debe usar el protocolo serviceport, el protocolo de red y los comandos serviceport ip.

Muestra el ejemplo

```
(new_cs1) #serviceport ip <ipaddr> <netmask> <gateway>
```

9. Opcionalmente, si el servidor TFTP está en un portátil, conecte el switch CN1610 al portátil mediante un cable Ethernet estándar y, a continuación, configure su puerto de red en la misma red con una dirección IP alternativa.

Puede utilizar el `ping` comando para verificar la dirección. Si no puede establecer la conectividad, debe utilizar una red no enrutada y configurar el puerto de servicio con IP 192,168.x o 172,16.x. Puede volver a configurar el puerto de servicio a la dirección IP de administración de producción en una fecha posterior.

10. De manera opcional, verifique e instale las versiones adecuadas del software RCF y FASTPATH para el nuevo switch. Si comprobó que el nuevo switch está configurado correctamente y no requiere actualizaciones del software RCF y FASTPATH, debería ir al paso 13.
 - a. Compruebe la nueva configuración del interruptor.

Muestra el ejemplo

```
(new_cs1) >*enable*  
(new_cs1) #show version
```

- b. Descargue el RCF en el nuevo switch.

Muestra el ejemplo

```
(new_cs1) #copy tftp://<server_ip_address>/CN1610_CS_RCF_v1.2.txt
nvram:script CN1610_CS_RCF_v1.2.scr
Mode.      TFTP
Set Server IP. 172.22.201.50
Path.      /
Filename.....
CN1610_CS_RCF_v1.2.txt
Data Type..... Config Script
Destination Filename.....
CN1610_CS_RCF_v1.2.scr
File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.

Management access will be blocked for the duration of the
transfer Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for
the duration of the transfer. please wait...
Validating configuration script...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script validated.
File transfer operation completed successfully.
```

- c. Compruebe que el RCF se ha descargado en el conmutador.

Muestra el ejemplo

```
(new_cs1) #script list
Configuration Script Nam    Size(Bytes)
-----
CN1610_CS_RCF_v1.1.scr      2191
CN1610_CS_RCF_v1.2.scr      2240
latest_config.scr           2356

4 configuration script(s) found.
2039 Kbytes free.
```

11. Aplique el RCF al interruptor CN1610.

Muestra el ejemplo

```
(new_cs1) #script apply CN1610_CS_RCF_v1.2.scr
Are you sure you want to apply the configuration script? (y/n) y
...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script 'CN1610_CS_RCF_v1.2.scr' applied. Note that the
script output will go to the console.
After the script is applied, those settings will be active in the
running-config file. To save them to the startup-config file, you
must use the write memory command, or if you used the reload answer
yes when asked if you want to save the changes.
```

- a. Guarde el archivo de configuración en ejecución para que se convierta en el archivo de configuración de inicio cuando reinicie el conmutador.

Muestra el ejemplo

```
(new_cs1) #write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved!
```

- b. Descargue la imagen en el switch CN1610.

Muestra el ejemplo

```
(new_cs1) #copy
tftp://<server_ip_address>/NetApp_CN1610_1.2.0.7.stk active
Mode.    TFTP
Set Server IP.  tftp_server_ip_address
Path.    /
Filename.....
NetApp_CN1610_1.2.0.7.stk
Data Type.  Code
Destination Filename.  active

Management access will be blocked for the duration of the
transfer

Are you sure you want to start? (y/n) y

TFTP Code transfer starting...

File transfer operation completed successfully.
```

- c. Ejecute la nueva imagen de inicio activa reiniciando el conmutador.

El conmutador debe reiniciarse para que el comando del paso 6 refleje la nueva imagen. Hay dos vistas posibles para una respuesta que puede ver después de introducir el comando reload.

Muestra el ejemplo

```
(new_cs1) #reload
The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved! System will now restart!
.
.
.
Cluster Interconnect Infrastructure

User:admin Password: (new_cs1) >*enable*
```

- a. Copie el archivo de configuración guardado del interruptor antiguo al nuevo.

Muestra el ejemplo

```
(new_cs1) #copy tftp://<server_ip_address>/<filename>.scr  
nvram:script <filename>.scr
```

- b. Aplique la configuración guardada anteriormente al nuevo conmutador.

Muestra el ejemplo

```
(new_cs1) #script apply <filename>.scr  
Are you sure you want to apply the configuration script? (y/n) y  
  
The system has unsaved changes.  
Would you like to save them now? (y/n) y  
  
Config file 'startup-config' created successfully.  
  
Configuration Saved!
```

- c. Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.

Muestra el ejemplo

```
(new_cs1) #write memory
```

12. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport: `system node autosupport invoke -node * -type all - message MAINT=xh`

x es la duración de la ventana de mantenimiento en horas.



El mensaje de AutoSupport notifica al soporte técnico de esta tarea de mantenimiento para que la creación automática de casos se suprima durante la ventana de mantenimiento.

13. En el nuevo switch new_CS1, inicie sesión como el usuario administrador y apague todos los puertos que están conectados a las interfaces de clúster de nodos (puertos 1 a 12).

Muestra el ejemplo

```
User:*admin*
Password:
(new_cs1) >*enable*
(new_cs1) #

(new_cs1) config
(new_cs1) (config) interface 0/1-0/12
(new_cs1) (interface 0/1-0/12) shutdown
(new_cs1) (interface 0/1-0/12) exit
(new_cs1) #write memory
```

14. Migre los LIF del clúster desde los puertos conectados al switch OLD_CS1.

Debe migrar cada LIF de clúster desde la interfaz de gestión de su nodo actual.

Muestra el ejemplo

```
cluster::> set -privilege advanced
cluster::> network interface migrate -vserver <vserver_name> -lif
<Cluster_LIF_to_be_moved> - sourcenode <current_node> -dest-node
<current_node> -dest-port <cluster_port_that_is_UP>
```

15. Compruebe que todas las LIF de clúster se han movido al puerto de clúster adecuado en cada nodo.

Muestra el ejemplo

```
cluster::> network interface show -role cluster
```

16. Apague los puertos de clúster conectados al switch que reemplazó.

Muestra el ejemplo

```
cluster::*> network port modify -node <node_name> -port
<port_to_admin_down> -up-admin false
```

17. Compruebe el estado del clúster.

Muestra el ejemplo

```
cluster::*> cluster show
```

18. Compruebe que los puertos están inactivos.

Muestra el ejemplo

```
cluster::*> cluster ping-cluster -node <node_name>
```

19. En el switch CS2, apague los puertos ISL 13 a 16.

Muestra el ejemplo

```
(cs2) config  
(cs2)(config) interface 0/13-0/16  
(cs2)(interface 0/13-0/16) #shutdown  
(cs2) #show port-channel 3/1
```

20. Verificar si el administrador de almacenamiento está preparado para reemplazar el switch.
21. Quite todos los cables del switch old_CS1 y, a continuación, conecte los cables a los mismos puertos del switch NEW_CS1.
22. En el switch CS2, levante los puertos ISL de 13 a 16.

Muestra el ejemplo

```
(cs2) config  
(cs2)(config) interface 0/13-0/16  
(cs2)(interface 0/13-0/16) #no shutdown
```

23. Abra los puertos en el nuevo switch que están asociados con los nodos del clúster.

Muestra el ejemplo

```
(cs2) config  
(cs2)(config) interface 0/1-0/12  
(cs2)(interface 0/13-0/16) #no shutdown
```

24. En un solo nodo, abra el puerto de nodo del clúster que está conectado al switch sustituido y, a continuación, confirme que el enlace está activo.

Muestra el ejemplo

```
cluster::*> network port modify -node node1 -port  
<port_to_be_onlined> -up-admin true  
cluster::*> network port show -role cluster
```

25. Revierta los LIF del clúster que están asociados con el puerto en el paso 25 en el mismo nodo.

En este ejemplo, las LIF de node1 se revierten correctamente si la columna «is Home» es verdadera.

Muestra el ejemplo

```
cluster::*> network interface revert -vserver node1 -lif  
<cluster_lif_to_be_reverted>  
cluster::*> network interface show -role cluster
```

26. Si el LIF de clúster del primer nodo está activo y se vuelve a convertir a su puerto de inicio, repita los pasos 25 y 26 para abrir los puertos del clúster y para revertir las LIF de clúster en los demás nodos del clúster.
27. Muestre información acerca de los nodos del clúster.

Muestra el ejemplo

```
cluster::*> cluster show
```

28. Confirme que el archivo de configuración de inicio y el archivo de configuración en ejecución son correctos en el conmutador sustituido. Este archivo de configuración debe coincidir con la salida del paso 1.

Muestra el ejemplo

```
(new_cs1) >*enable*  
(new_cs1) #show running-config  
(new_cs1) #show startup-config
```

29. Si ha suprimido la creación automática de casos, vuelva a habilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Sustituya los switches de clúster CN1610 de NetApp por conexiones sin switches

Puede migrar desde un clúster con una red de clúster conmutada a uno donde dos nodos están conectados directamente para ONTAP 9.3 y versiones posteriores.

Revise los requisitos

Directrices

Revise las siguientes directrices:

- La migración a una configuración de clúster de dos nodos sin switch es una operación no disruptiva. La mayoría de los sistemas tienen dos puertos de interconexión de clúster dedicados en cada nodo, pero también puede usar este procedimiento para sistemas con un número mayor de puertos de interconexión de clúster dedicados en cada nodo, como cuatro, seis u ocho.
- No se puede usar la función de interconexión de clúster sin switches con más de dos nodos.
- Si tiene un clúster de dos nodos existente que utiliza switches de interconexión de clúster y ejecuta ONTAP 9.3 o una versión posterior, puede reemplazar los switches por conexiones directas de vuelta a atrás entre los nodos.

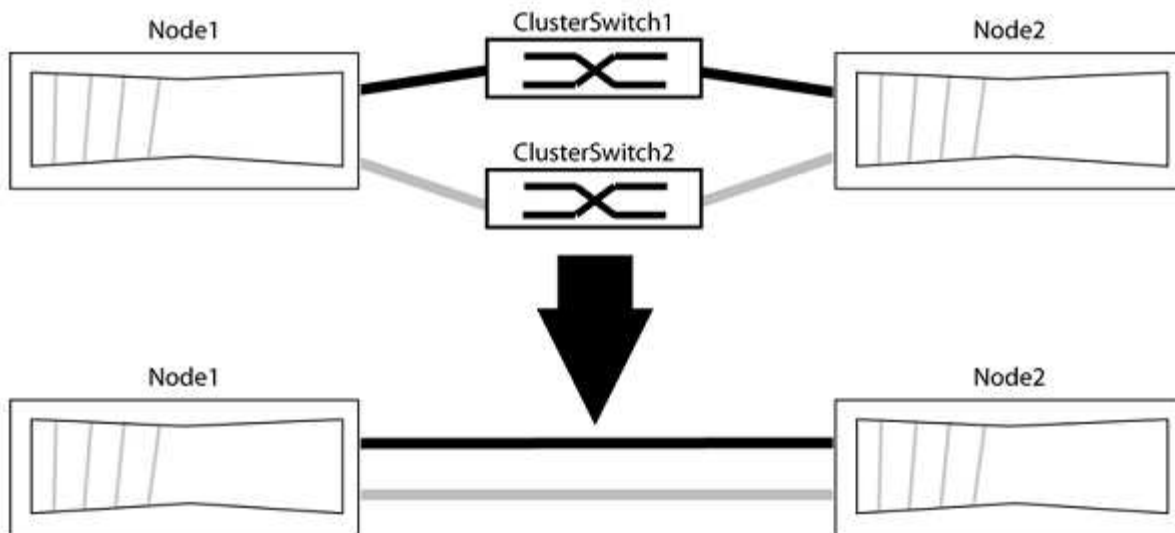
Lo que necesitará

- Un clúster en buen estado que consta de dos nodos conectados por switches de clúster. Los nodos deben ejecutar la misma versión de ONTAP.
- Cada nodo con el número requerido de puertos de clúster dedicados, que proporcionan conexiones redundantes de interconexión de clúster para admitir la configuración de su sistema. Por ejemplo, hay dos puertos redundantes para un sistema con dos puertos de Cluster Interconnect dedicados en cada nodo.

Migrar los switches

Acerca de esta tarea

En el siguiente procedimiento, se quitan los switches de clúster de dos nodos y se reemplaza cada conexión al switch por una conexión directa al nodo compañero.



Acerca de los ejemplos

Los ejemplos del siguiente procedimiento muestran nodos que utilizan «e0a» y «e0b» como puertos del clúster. Sus nodos pueden usar distintos puertos de clúster según varían según el sistema.

Paso 1: Preparación para la migración

1. Cambie el nivel de privilegio a Advanced, introduzca `y` cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado `*>` aparece.

2. ONTAP 9.3 y versiones posteriores admiten la detección automática de clústeres sin switch, que está habilitado de forma predeterminada.

Puede verificar que la detección de clústeres sin switch esté habilitada mediante el comando de privilegio avanzado:

```
network options detect-switchless-cluster show
```

Muestra el ejemplo

El siguiente resultado de ejemplo muestra si la opción está habilitada.

```
cluster::*> network options detect-switchless-cluster show
(network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Si la opción "Activar detección de clústeres sin switch" es `false` Póngase en contacto con el soporte de NetApp.

3. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

donde `h` es la duración del plazo de mantenimiento en horas. El mensaje notifica al soporte técnico de esta tarea de mantenimiento para que estos puedan impedir la creación automática de casos durante la ventana de mantenimiento.

En el ejemplo siguiente, el comando suprime la creación automática de casos durante dos horas:

Muestra el ejemplo

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Paso 2: Configure los puertos y el cableado

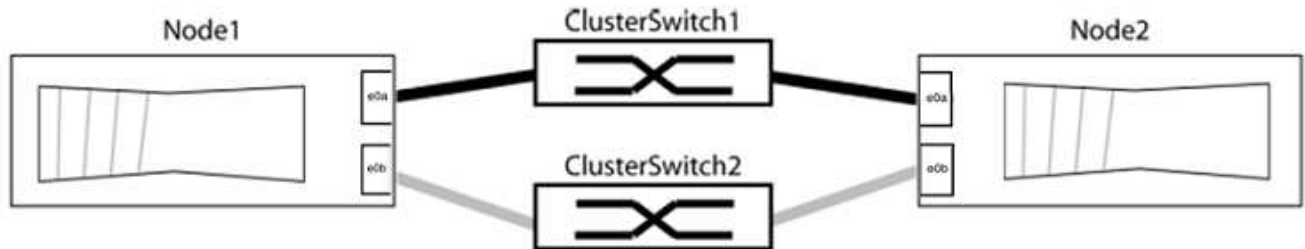
1. Organice los puertos del clúster en cada switch en grupos de modo que los puertos del clúster en `group1` vayan a Cluster switch1 y los puertos del cluster en `group2` vayan a cluster switch2. Estos grupos son

necesarios más adelante en el procedimiento.

2. Identificar los puertos del clúster y verificar el estado y el estado del enlace:

```
network port show -ipspace Cluster
```

En el siguiente ejemplo, en el caso de nodos con puertos de clúster "e0a" y "e0b", un grupo se identifica como "1:e0a" y "2:e0a" y el otro grupo como "1:e0b" y "2:e0b". Sus nodos pueden usar puertos de clúster diferentes porque varían según el sistema.



Compruebe que los puertos tienen un valor de `up` Para la columna "Link" y un valor de `healthy` Para la columna "Estado de salud".

Muestra el ejemplo

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
Speed (Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
-----
-----
e0a Cluster Cluster up 9000 auto/10000 healthy
false
e0b Cluster Cluster up 9000 auto/10000 healthy
false

Node: node2

Ignore
Speed (Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
-----
-----
e0a Cluster Cluster up 9000 auto/10000 healthy
false
e0b Cluster Cluster up 9000 auto/10000 healthy
false
4 entries were displayed.
```

3. Confirmar que todas las LIF de clúster están en sus puertos raíz.

Compruebe que la columna "es-home" es true Para cada LIF del clúster:

```
network interface show -vserver Cluster -fields is-home
```

Muestra el ejemplo

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif           is-home
-----  -
Cluster  node1_clus1   true
Cluster  node1_clus2   true
Cluster  node2_clus1   true
Cluster  node2_clus2   true
4 entries were displayed.
```

Si hay LIF de clúster que no estén en sus puertos raíz, revierte estos LIF a sus puertos principales:

```
network interface revert -vserver Cluster -lif *
```

4. Deshabilite la reversión automática para las LIF del clúster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Compruebe que todos los puertos enumerados en el paso anterior están conectados a un conmutador de red:

```
network device-discovery show -port cluster_port
```

La columna “dispositivo detectado” debe ser el nombre del conmutador de clúster al que está conectado el puerto.

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster «e0a» y «e0b» están conectados correctamente a los switches del clúster «cs1» y «cs2».

```
cluster::> network device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e0a    cs1                      0/11       BES-53248
          e0b    cs2                      0/12       BES-53248
node2/cdp
          e0a    cs1                      0/9        BES-53248
          e0b    cs2                      0/9        BES-53248
4 entries were displayed.
```


6. Compruebe la conectividad del clúster:

```
cluster ping-cluster -node local
```

7. Compruebe que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

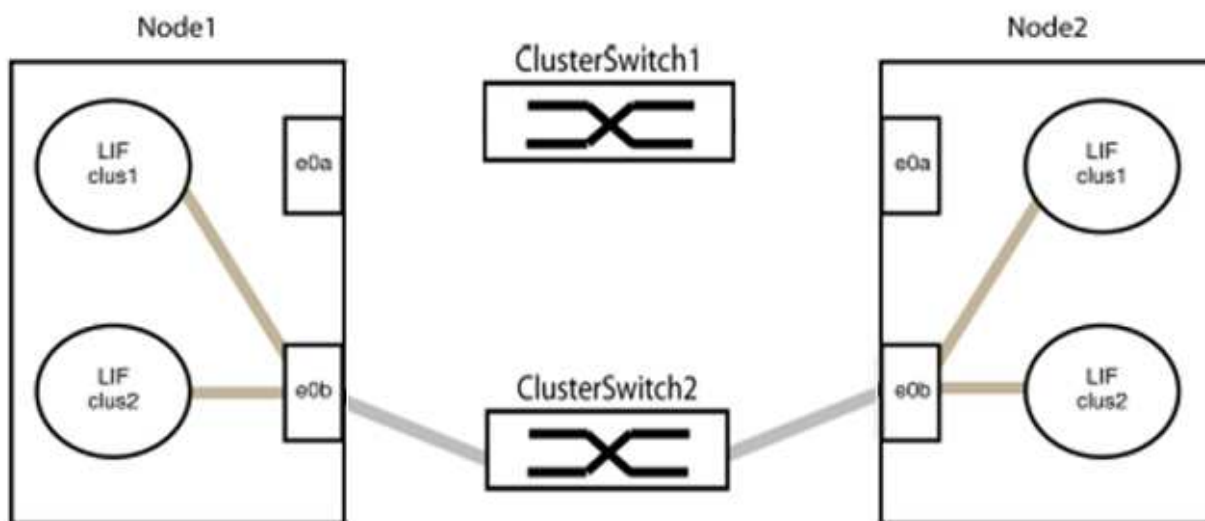
8. Configure la configuración sin switches para los puertos del grupo 1.



Para evitar posibles problemas de red, debe desconectar los puertos del grupo 1 y volver a conectarlos lo antes posible, por ejemplo, **en menos de 20 segundos**.

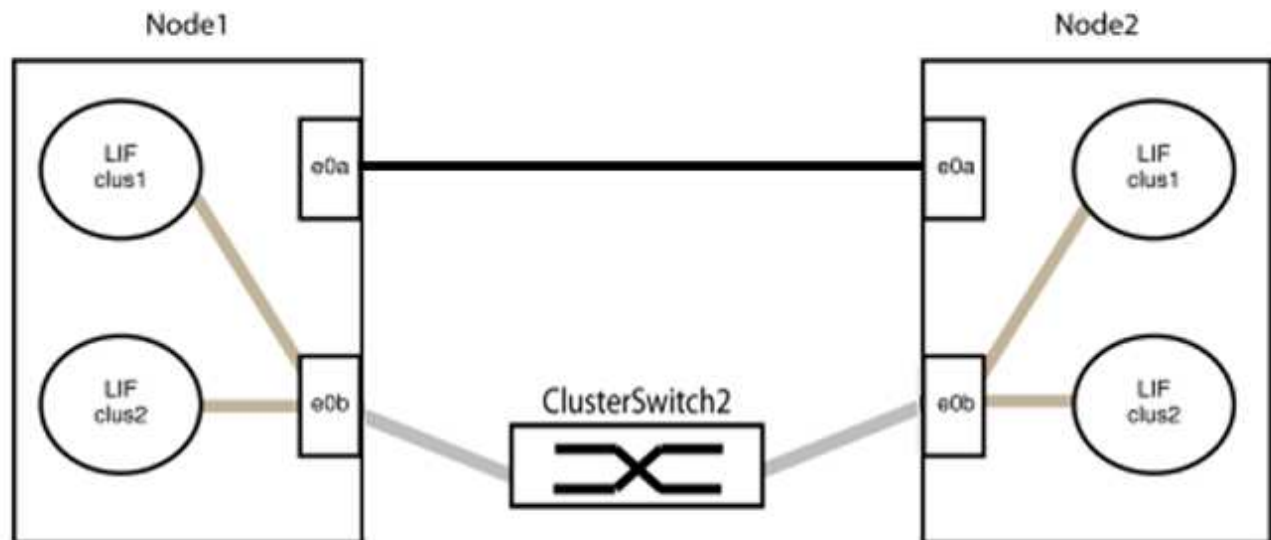
a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

En el ejemplo siguiente, los cables se desconectan del puerto "e0a" en cada nodo, y el tráfico del clúster continúa a través del switch y el puerto "e0b" en cada nodo:



b. Conecte los puertos en group1 de vuelta a espalda.

En el siguiente ejemplo, "e0a" en el nodo 1 está conectado a "e0a" en el nodo 2:



9. La opción de red de clúster sin switch desde la transición `false` para `true`. Esto puede tardar hasta 45 segundos. Confirme que la opción sin switches está establecida en `true`:

```
network options switchless-cluster show
```

En el siguiente ejemplo se muestra que el clúster sin switch está habilitado:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

10. Compruebe que la red de clúster no se haya interrumpido:

```
cluster ping-cluster -node local
```



Antes de continuar con el siguiente paso, debe esperar al menos dos minutos para confirmar una conexión de retroceso en funcionamiento en el grupo 1.

11. Configure la configuración sin switches para los puertos del grupo 2.



Para evitar posibles problemas de red, debe desconectar los puertos del grupo 2 y volver a conectarlos lo antes posible, por ejemplo, **en menos de 20 segundos**.

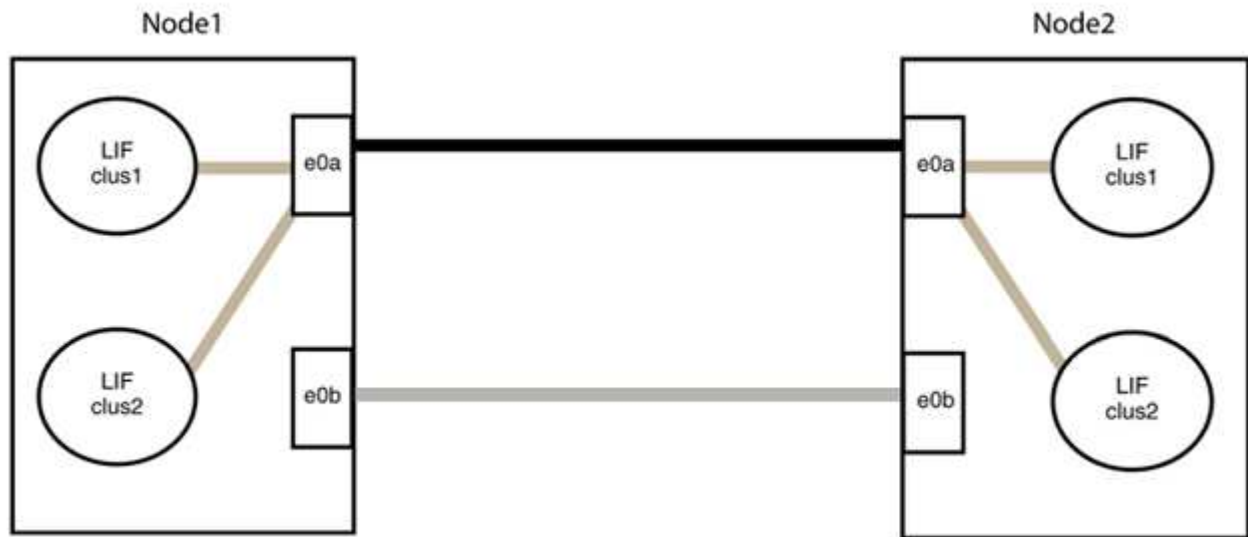
- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

En el ejemplo siguiente, los cables se han desconectado del puerto "e0b" en cada nodo y el tráfico del clúster continúa por la conexión directa entre los puertos "e0a":



b. Conecte los puertos en group2 de vuelta a back.

En el ejemplo siguiente, hay conectado "e0a" en el nodo 1 a "e0a" en el nodo 2 y "e0b" en el nodo 1 está conectado a "e0b" en el nodo 2:



Paso 3: Verificar la configuración

1. Compruebe que los puertos de ambos nodos están conectados correctamente:

```
network device-discovery show -port cluster_port
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos de clúster «e0a» y «e0b» están conectados correctamente al puerto correspondiente del partner de clúster:

```
cluster::> net device-discovery show -port e0a|e0b
(network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
           e0a    node2                      e0a        AFF-A300
           e0b    node2                      e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                      e0a        AFF-A300
           e0b    node1                      e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Volver a habilitar la reversión automática para las LIF del clúster:

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

3. Compruebe que todas las LIF son Home. Esto puede tardar unos segundos.

```
network interface show -vserver Cluster -lif lif_name
```

Muestra el ejemplo

Los LIF se han revertido si la columna “es de inicio” es true, como se muestra para node1_clus2 y.. node2_clus2 en el siguiente ejemplo:

```
cluster::> network interface show -vserver Cluster -fields curr-  
port,is-home  
vserver  lif                curr-port is-home  
-----  -  
Cluster  node1_clus1         e0a      true  
Cluster  node1_clus2         e0b      true  
Cluster  node2_clus1         e0a      true  
Cluster  node2_clus2         e0b      true  
4 entries were displayed.
```

Si alguna LIFS de cluster no ha regresado a sus puertos de directorio raíz, revierta manualmente desde el nodo local:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Compruebe el estado del clúster de los nodos desde la consola del sistema de cualquier nodo:

```
cluster show
```

Muestra el ejemplo

En el siguiente ejemplo se muestra *epsilon* en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true      false  
node2 true    true      false  
2 entries were displayed.
```

5. Confirme la conectividad entre los puertos del clúster:

```
cluster ping-cluster local
```

6. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Para obtener más información, consulte ["Artículo de la base de conocimientos de NetApp 1010449: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#).

7. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.