



Documentación de conmutadores para sistemas de hardware ONTAP

Install and maintain

NetApp
October 24, 2025

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems-switches/index.html> on October 24, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de conmutadores para sistemas de hardware ONTAP	1
Manos a la obra	2
Novedades para los switches	2
Nuevo soporte de conmutador	2
Obtenga información sobre los sistemas AFX, clúster, almacenamiento y conmutadores compartidos	3
Conmutadores de sistemas AFX	3
Switches de clúster	4
Switches de almacenamiento	4
Switches compartidos	4
Fin de la disponibilidad	4
Póngase en funcionamiento con sistemas AFX, clúster, almacenamiento y conmutadores compartidos	4
Conmutadores de sistemas AFX	7
Cisco Nexus 9332D-GX2B	7
Manos a la obra	7
Instale el hardware	10
Configurar el software	10
Reemplazar un conmutador Cisco Nexus 9332D-GX2B	121
Cisco Nexus 9364D-GX2A	149
Manos a la obra	149
Instale el hardware	152
Configurar el software	153
Reemplazar un conmutador Cisco Nexus 9364D-GX2A	280
Switches de clúster	309
BES-53248 compatible con Broadcom	309
Manos a la obra	309
Instale el hardware	313
Configurar el software	316
Actualizar el conmutador	414
Migrar los switches	458
Reemplace los interruptores	494
Cisco Nexus 9336C-FX2 o 9336C-FX2-T	523
Manos a la obra	523
Instale el hardware	529
Configurar el software	540
Migrar los switches	611
Reemplace los interruptores	664
NVIDIA SN2100	697
Manos a la obra	697
Instale el hardware	700
Configurar el software	709
Migrar los switches	785
Reemplace los interruptores	841
Switches de almacenamiento	876

Cisco Nexus 9336C-FX2 o 9336C-FX2-T	876
Manos a la obra	876
Instale el hardware	881
Configurar el software	891
Reemplace los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T	935
NVIDIA SN2100	941
Manos a la obra	941
Instale el hardware	944
Configurar el software	953
Migrar switches	984
Sustituya el conmutador de almacenamiento NVIDIA SN2100	995
Switches compartidos	1003
Cisco Nexus 9336C-FX2	1003
Manos a la obra	1003
Instale el hardware	1005
Configurar el software	1014
Migrar switches	1082
Sustituya un switch compartido Cisco Nexus 9336C-FX2	1121
Supervise el estado del interruptor	1140
Descripción general del monitor de estado del switch	1140
Configure la supervisión de estado del switch	1140
Información general de configuración	1140
Configure la recopilación de registros	1140
Opcional: Configure SNMPv3 para su switch	1147
Compruebe el estado del interruptor	1165
Información general de la comprobación del estado	1165
Gestionar la supervisión de switches Ethernet	1165
Compruebe la supervisión de los conmutadores Ethernet	1167
Solucionar problemas de alertas	1168
Recopilación de registros	1168
Descripción general de la recopilación de registros	1168
Solución de problemas de recopilación de registros	1168
Switches de fin de disponibilidad	1170
Fin de la disponibilidad	1170
Anuncios de fin de venta y fin de vida útil	1170
Cisco Nexus 3232C	1170
Manos a la obra	1170
Instale el hardware	1173
Configurar el software	1183
Migrar switches	1240
Sustituya los interruptores	1337
Cisco Nexus 3132Q-V	1379
Manos a la obra	1379
Instale el hardware	1383
Configurar el software	1388

Migrar switches	1445
Sustituya los interruptores	1547
Cisco Nexus 92300YC	1593
Manos a la obra	1593
Instale el hardware	1598
Configurar el software	1610
Migrar switches	1651
Sustituya los interruptores	1689
CN1610 de NetApp	1721
Descripción general de la instalación y la configuración de los switches CN1610 de NetApp	1721
Instalar y configurar el flujo de trabajo de los switches CN1610 de NetApp	1722
Requisitos de documentación para los switches CN1610 de NetApp	1722
Instalar y configurar	1723
Migrar switches	1759
Sustituya los interruptores	1787
Avisos legales	1813
Derechos de autor	1813
Marcas comerciales	1813
Estadounidenses	1813
Política de privacidad	1813

Documentación de conmutadores para sistemas de hardware ONTAP

Manos a la obra

Novedades para los switches

Obtenga más información sobre los nuevos switches para los sistemas FAS y AFF. Para obtener información adicional sobre el interruptor, consulte la ["Hardware Universe de NetApp"](#).

Nuevo soporte de conmutador

Interruptores	Descripción	Comienzo disponible
Conmutador Cisco de 32 puertos 400 GbE (X190300-CS-PI y X190300-PE)	Compatibilidad con conmutadores Cisco 9332D-GX2B intra-clúster/HA/almacenamiento.	ONTAP 9.17.1
Conmutador Cisco de 64 puertos 400 GbE (X190310-CS-PI)	Compatibilidad con conmutadores Cisco 9364D-GX2A intra-clúster/HA/almacenamiento.	ONTAP 9.17.1
Conmutador de clúster y almacenamiento Cisco Nexus 9336C-FX2-T de 12 puertos 10/25/40/100 GbE (X190212-CS-PE y X190212-CS-PI)	Admite configuraciones de clúster de 10/25/40/100 GbE y configuraciones de almacenamiento de 100 GbE (almacenamiento conectado a conmutador).	ONTAP 9.10.1
Conmutador de clúster y almacenamiento Cisco Nexus 9336C-FX2-T de 12 puertos 10/25/40/100 GbE (X190212-CS-PE y X190212-CS-PI)	Admite configuraciones de clúster de 10/25/40/100 GbE y configuraciones de almacenamiento de 100 GbE (almacenamiento conectado a conmutador).	ONTAP 9.10.1
Switch NVIDIA de 16 puertos (X190006-PE y X190006-PI) de 100GbE Gb	Compatibilidad con switch de interconexión de clúster y switch de almacenamiento NVIDIA SN2100, incluida la compatibilidad con configuraciones IP de MetroCluster.	ONTAP 9.10.1
Switch Cisco de 36 puertos (X190200-CS-PE y X190200-CS-PI) de 100GbE Gb	Admite una infraestructura compartida (clúster, alta disponibilidad y almacenamiento conectado a switches) en la misma pareja de switches Cisco Nexus 9336C-FX2, incluida la compatibilidad con configuraciones de IP de MetroCluster.	ONTAP 9.9.1

Interruptores	Descripción	Comienzo disponible
Switch Cisco 100GbE de 36 puertos (X190200-CS-PE y X190200-CS-PI), (X190210-FE-PE y X190210-FE-PI)	Soporte del switch de interconexión de clúster Nexus 9336C-FX2 de Cisco y los switches de almacenamiento para sistemas de almacenamiento AFF y ASA, así como para la conectividad de datos de interfaz.	ONTAP 9.8
Conmutador Broadcom BES-53248 (X190005 y X190005R)	Compatibilidad con switches de interconexión de clúster BES-53248 de Broadcom para controladoras AFF/FAS con puertos 10/25GbE y 40/100GbE.	ONTAP 9.8
Switch Cisco de 36 puertos (X190200) y switch Cisco de 100GbE 100GbE Gb con 32 puertos (X190100 y X190100R)	Compatibilidad con switches de almacenamiento Nexus 3232C de Cisco para conectar bandejas de unidades NVMe de NS224 TB sistemas de almacenamiento AFF y ASA: • ASA A800/AFF A800 de AFF • ASA A700/AFF de AFF • AFF A400/AFF ASA A400 • AFF A320	ONTAP 9.8

Obtenga información sobre los sistemas AFX, clúster, almacenamiento y conmutadores compartidos

NetApp ofrece sistemas AFX, clústeres, almacenamiento y conmutadores compartidos que brindan comunicaciones internas con la capacidad de mover datos e interfaces de red sin interrupciones en todo el clúster.

Los switches de «front-end» proporcionan conectividad al almacenamiento host, mientras que los switches de clúster de «back-end» proporcionan conexiones entre dos o más controladoras de NetApp.



Solo se admiten switches back-end validados por NetApp (solicitados a NetApp).

Conmutadores de sistemas AFX

Los conmutadores de sistemas AFX le permiten crear conmutadores de red rápidos, energéticamente eficientes y que ahorran espacio. Su pequeño tamaño y alta densidad de puertos los hacen ideales para manejar redes grandes. Los puertos admiten diferentes velocidades y se pueden dividir en múltiples conexiones. Los conmutadores de sistemas AFX compatibles con NetApp incluyen:

- Cisco Nexus 9332D-GX2B
- Cisco Nexus 9364D-GX2A

Switches de clúster

Los switches de clúster permiten crear clústeres de ONTAP con más de dos nodos. Los switches de clúster admitidos por NetApp incluyen:

- Broadcom BES-53248
- Cisco Nexus 9336C-FX2
- NVIDIA SN2100

Switches de almacenamiento

Los switches de almacenamiento le permiten enrutar datos entre servidores y matrices de almacenamiento en una red DE área de almacenamiento (SAN). Algunos de los switches de almacenamiento compatibles con NetApp son:

- Cisco Nexus 9336C-FX2
- NVIDIA SN2100

Switches compartidos

Los switches compartidos permiten combinar la funcionalidad de clúster y almacenamiento en una configuración de switch compartido, al admitir el uso de RCF de almacenamiento y clúster compartidos. El switch compartido compatible con NetApp es:

- Cisco Nexus 9336C-FX2

Fin de la disponibilidad

Los siguientes switches de almacenamiento ya no se pueden adquirir, pero siguen siendo compatibles:

- Cisco Nexus 3232C
- Cisco Nexus 3132Q-V
- Cisco Nexus 92300YC
- CN1610 de NetApp

Póngase en funcionamiento con sistemas AFX, clúster, almacenamiento y conmutadores compartidos

Para comenzar a trabajar con sistemas AFX, clústeres, almacenamiento y conmutadores compartidos, debe instalar componentes de hardware y configurar su conmutador.

La implementación del switch implica el siguiente flujo de trabajo.



Instale la tornillería del interruptor

Instale los switches en el rack o armario. Acceda a las siguientes instrucciones para su modelo de conmutador.

Conmutadores de sistemas AFX • "Instalar el conmutador Cisco Nexus 9332D-GX2B" • "Instalar el conmutador Cisco Nexus 9364D-GX2A"	Switches de clúster • "Instale el conmutador BES-53248" • "Instale el switch Cisco Nexus 9336C-FX2" • "Instale el conmutador NVIDIA SN2100"	Switches de almacenamiento • "Instale el switch Cisco Nexus 9336C-FX2" • "Instale el conmutador NVIDIA SN2100"	Switches compartidos • "Instale el switch Cisco Nexus 9336C-FX2"

2

Instale el sistema de almacenamiento y las bandejas de almacenamiento

Instale el sistema de almacenamiento y las bandejas de almacenamiento en el armario o rack. Acceda a las instrucciones de instalación y configuración para el modelo de plataforma.

• "Sistemas AFX" • "Sistemas AFF" • "Sistemas ASA" • "Sistemas ASA r2" • "Sistemas FAS"			

3

Conecte los interruptores a los controladores

Las instrucciones de instalación y configuración de los sistemas ONTAP incluyen instrucciones para cablear los puertos de la controladora al switch. Sin embargo, si necesita listas de cables y transceptores admitidos e información detallada sobre los puertos de host para el switch, acceda a las siguientes instrucciones para su modelo de switch.

Conmutadores de sistemas AFX • "Cablee el conmutador Cisco Nexus 9332D-GX2B" • "Cablee el conmutador Cisco Nexus 9364D-GX2A"	Switches de clúster • "Conecte el interruptor BES-53248" • "Cablee el conmutador Cisco Nexus 9336C-FX2" • "Cablee el conmutador NVIDIA SN2100"	Switches de almacenamiento • "Cablee el conmutador Cisco Nexus 9336C-FX2" • "Cablee el conmutador NVIDIA SN2100"	Switches compartidos • "Cablee el conmutador Cisco Nexus 9336C-FX2"

4

Configurar el software del conmutador

Para instalar y configurar el software en el conmutador, siga el flujo de trabajo de instalación de software del

modelo de conmutador.

Conmutadores de sistemas AFX • "Instalar software para el conmutador Cisco Nexus 9332D-GX2B" • "Instalar software para el conmutador Cisco Nexus 9364D-GX2A"	Switches de clúster • "Instale el software para los conmutadores BES-53248" • "Instale el software del switch Cisco Nexus 9336C-FX2" • "Instale el software para el conmutador NVIDIA SN2100"	Switches de almacenamiento • "Instale el software del switch Cisco Nexus 9336C-FX2" • "Instale el software para el conmutador NVIDIA SN2100"	Switches compartidos • "Instale el software del switch Cisco Nexus 9336C-FX2"

5

Configuración completa del sistema

Después de configurar los switches e instalar el software requerido, acceda a las instrucciones de instalación y configuración para el modelo de plataforma de sistemas ONTAP y complete la configuración del sistema.

• "Sistemas AFX" • "Sistemas AFF" • "Sistemas ASA" • "Sistemas ASA r2" • "Sistemas FAS"			

6

Configuración completa de ONTAP

Después de instalar y configurar las controladoras y los switches de los sistemas ONTAP, debe completar la configuración del almacenamiento en ONTAP. Acceda a las siguientes instrucciones de acuerdo con la configuración de la implementación.

- Para implementaciones de ONTAP, consulte "Configure ONTAP".
- Para ver ONTAP con implementaciones de MetroCluster, consulte "Configuración de MetroCluster con ONTAP".

Conmutadores de sistemas AFX

Cisco Nexus 9332D-GX2B

Manos a la obra

Flujo de trabajo de instalación y configuración para los conmutadores Cisco 9332D-GX2B

El conmutador Cisco 9332D-GX2B es parte de la plataforma Cisco Nexus 9000. Los conmutadores de sistemas AFX le permiten crear clústeres ONTAP con más de dos nodos.

Siga estos pasos de flujo de trabajo para instalar y configurar sus conmutadores Cisco 9332D-GX2B.

1

"Revisar los detalles del puerto del conmutador"

Revise los detalles del puerto del conmutador Cisco 9332D-GX2B.

2

"Revisar la documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores 9332D-GX2B y el clúster ONTAP .

3

"Revisar los requisitos de Smart Call Home"

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

4

"Instale el hardware"

Instale el hardware del interruptor.

5

"Configurar el software"

Configurar el software del conmutador.

Detalles del puerto para los conmutadores Cisco Nexus 9332D-GX2B

El conmutador Cisco Nexus 9332D-GX2B es parte de la plataforma Cisco Nexus 9000. Los conmutadores del sistema AFX le permiten crear clústeres ONTAP con más de dos nodos.

Detalles del puerto del Cisco Nexus 9332D-GX2B

Puertos	Descripción
Ethernet1/1/1-4 a Ethernet1/30/1-4	Modo 4x100GbE para conexiones de clúster, alta disponibilidad y almacenamiento
Ethernet1/31, Ethernet1/32	400GbE ISL

Ver el ["Hardware Universe"](#) para obtener detalles de los puertos utilizados por la plataforma.

Requisitos de documentación para los conmutadores Cisco Nexus 9332D-GX2B

Para la instalación y el mantenimiento del conmutador Cisco Nexus 9332D-GX2B, asegúrese de revisar la documentación específica del conmutador y del controlador para configurar los conmutadores 9332D-GX2B y el clúster ONTAP .

Documentación de los switches

Para configurar los conmutadores Cisco Nexus 9332D-GX2B, necesita la siguiente documentación del ["Compatibilidad con los switches Cisco Nexus serie 9000"](#) página:

Título del documento	Descripción
"Guía de instalación del hardware del conmutador de modo NX-OS Cisco Nexus 9332D-GX2B"	Proporciona información detallada acerca de los requisitos del sitio, detalles del switch de hardware y las opciones de instalación.
"Guías de configuración del software del switch Cisco Nexus serie 9000" (seleccione la guía para la versión de NX-OS instalada en sus conmutadores)	Proporciona la información inicial de configuración del switch que necesita para poder configurar el switch para el funcionamiento de ONTAP.
"Guía de actualización y degradación del software Cisco Nexus serie 9000 NX-OS" (seleccione la guía para la versión de NX-OS instalada en sus conmutadores)	Proporciona información sobre cómo degradar el switch a software de switch compatible con ONTAP, si es necesario.
"Referencia de comandos NX-OS de Cisco Nexus serie 9000"	Proporciona vínculos a las diferentes referencias de comandos proporcionadas por Cisco.
"Referencia de mensajes del sistema NX-OS de Cisco Nexus serie 9000"	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.

Título del documento	Descripción
"Notas de la versión de Cisco Nexus serie 9000 NX-OS" (seleccione las notas para la versión de NX-OS instalada en sus conmutadores)	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 de la ["Centro de documentación de ONTAP 9"](#) .

Nombre	Descripción
"Documentación de los sistemas AFX"	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.

Requisitos de Smart Call Home

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

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

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

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

- Debe haber un servidor de correo electrónico.
- 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

Ir a la ["Flujo de trabajo de instalación y configuración de AFX"](#) para aprender cómo instalar y configurar el hardware del conmutador y el hardware del controlador para su sistema.

La documentación de instalación y configuración de AFX incluye información como:

- Instrucciones para preparar el sitio, desempacar las cajas y comparar el contenido de las cajas con el albarán, y registrar el sistema para acceder a los beneficios de soporte.
- Instrucciones para instalar los conmutadores, controladores y estantes de almacenamiento en un gabinete NetApp o un rack de telecomunicaciones.
- Instrucciones para cablear su sistema, incluido el cableado del almacenamiento del controlador para cambiar las conexiones y el cableado del estante para cambiar las conexiones.

Configurar el software

Configurar el flujo de trabajo del software para los conmutadores Cisco 9332D-GX2B

Para instalar y configurar el software de un conmutador Cisco 9332D-GX2B e instalar o actualizar el archivo de configuración de referencia (RCF), siga estos pasos:

1

["Configurar el conmutador 9332D-GX2B"](#)

Configurar el conmutador Cisco 9332D-GX2B.

2

["Prepárese para instalar el software NX-OS y RCF"](#)

Instale el software Cisco NX-OS y los archivos de configuración de referencia (RCF) en los conmutadores Cisco 9332D-GX2B.

3

["Instale o actualice el software NX-OS"](#)

Descargue e instale o actualice el software NX-OS en el conmutador Cisco 9332D-GX2B.

4

["Instale o actualice el RCF"](#)

Instale o actualice el RCF después de configurar el conmutador Cisco 9332D-GX2B por primera vez. También puede utilizar este procedimiento para actualizar su versión de RCF.

5**"Verifique que SSH esté habilitado en los conmutadores Cisco 9332D-GX2B"**

Verifique que SSH esté habilitado en el conmutador Cisco 9332D-GX2B para su uso con el Monitor de estado del conmutador Ethernet (CSHM) y las funciones de recopilación de registros.

6**"Restablecer el interruptor a los valores predeterminados de fábrica"**

Borrar la configuración del conmutador Cisco 9332D-GX2B.

Una vez que haya terminado de configurar sus conmutadores, vaya a ["Encienda su sistema de almacenamiento AFX 1K"](#) .

Configurar el conmutador 9332D-GX2B

Siga este procedimiento para configurar el conmutador Cisco Nexus 9332D-GX2B.

Antes de empezar

Asegúrese de tener:

- Encienda sus interruptores.
- 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.



- NX-OS 10.4.2 es la única versión compatible con los conmutadores Cisco Nexus 9332D-GX2B en un clúster ONTAP .
- No actualice ni degrade su versión de NX-OS a una versión no compatible; actualmente solo se admite la versión 10.4.2.

- Las licencias aplicables, la información de configuración y red, y los cables.
- RCF de red compartida y red de administración de NetApp aplicables descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#) . Todos los conmutadores de red compartida y de red de administración de Cisco llegan con la configuración predeterminada de fábrica estándar de Cisco . Estos conmutadores también tienen la versión actual del software NX-OS pero no tienen los RCF cargados.
- ["Documentación necesaria sobre el switch y ONTAP"](#) .

Pasos

1. Realizar una configuración inicial de los conmutadores de red compartidos.

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.	Introduzca el nombre del switch, que 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
¿Habilitar el servicio telnet? (sí/no)	Responda con no . El valor predeterminado es no

Prompt	Respuesta
¿Servicio SSH habilitado? (sí/no)	Responda con sí. El valor predeterminado es yes.  Se recomienda SSH cuando se utiliza Ethernet Switch Health Monitor (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.
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 a 2048.
¿Configurar el servidor NTP? (sí/no)	Responda con no . El valor predeterminado es no
Configuración de 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)	Responda con sí para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.  Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador.

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

El futuro

Después de haber configurado sus conmutadores, "[Prepárese para instalar el software NX-OS y RCF](#)".

Prepárese para instalar el software NX-OS y RCF

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

Acerca de los ejemplos

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

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de los nodos son node1-01, node1-02, node1-03 y node1-04.
- Los nombres del clúster LIF son:
 - node1-01_clus1 y node1-01_clus2 para node1-01
 - node1-02_clus1 y node1-02_clus2 para node1-02
 - node1-03_clus1 y node1-03_clus2 para node1-03
 - node1-04_clus1 y node1-04_clus2 para node1-04
- 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.

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. Consulta el estado administrativo y operativo de cada puerto.

a. Puertos de clúster

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

```
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

node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e10b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e11a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e11b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e1a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	e1b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
	e7b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
node1-02/cdp			
	e10a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e10b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e11a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e11b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e1a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	e1b	cs2 (FDOXXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	.		
	.		
	.		
	e7a	cs1 (FLM284504N6)	Ethernet1/16/2

```
N9K-C9332D-GX2B
```

```
e7b
```

```
cs1 (FDO2846056X)
```

```
Ethernet1/16/2
```

```
N9K-C9332D-GX2B
```

```
.
```

```
.
```

```
.
```

ii. Mostrar los atributos del puerto de red:

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

Muestra el ejemplo

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

Node: node1-01

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000

```
healthy false
```

```
Node: nodel-04
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy false						
e7b	Cluster	Cluster		up	9000	auto/100000
healthy false						

```
8 entries were displayed.
```

iii. Mostrar información sobre los LIF del clúster:

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

```
8 entries were displayed.
```

b. Puertos HA

i. Mostrar información sobre los puertos HA:

```
ha interconnect status show -node <node-name>
```


Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

- i. Mostrar información sobre los puertos de almacenamiento:

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

Muestra el ejemplo

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

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

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

4. Verificar la conectividad de las interfaces del clúster remoto.

- Puedes utilizar el `network interface check cluster-connectivity show` Comando para mostrar los detalles de una verificación de accesibilidad para la conectividad del clúster:

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

Muestra el ejemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-02_clus1
none			
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-02_clus1
none			
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-01_clus1
none			
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-01_clus2
none			
.			
.			
.			

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

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node1-04
Getting addresses from network interface table...
Cluster node1-01_clus1 169.254.36.44 node1-01 e7a
Cluster node1-01_clus2 169.254.7.5 node1-01 e7b
Cluster node1-02_clus1 169.254.197.206 node1-02 e7a
Cluster node1-02_clus2 169.254.195.186 node1-02 e7b
Cluster node1-03_clus1 169.254.192.49 node1-03 e7a
Cluster node1-03_clus2 169.254.182.76 node1-03 e7b
Cluster node1-04_clus1 169.254.59.49 node1-04 e7a
Cluster node1-04_clus2 169.254.62.244 node1-04 e7b
Local = 169.254.59.49 169.254.62.244
Remote = 169.254.36.44 169.254.7.5 169.254.197.206 169.254.195.186
169.254.192.49 169.254.182.76
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 169.254.59.49 to Remote 169.254.182.76
    Local 169.254.59.49 to Remote 169.254.192.49
    Local 169.254.59.49 to Remote 169.254.195.186
    Local 169.254.59.49 to Remote 169.254.197.206
    Local 169.254.59.49 to Remote 169.254.36.44
    Local 169.254.59.49 to Remote 169.254.7.5
    Local 169.254.62.244 to Remote 169.254.182.76
    Local 169.254.62.244 to Remote 169.254.192.49
    Local 169.254.62.244 to Remote 169.254.195.186
    Local 169.254.62.244 to Remote 169.254.197.206
    Local 169.254.62.244 to Remote 169.254.36.44
    Local 169.254.62.244 to Remote 169.254.7.5
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)
```

5. Verifique que el comando de reversión automática esté habilitado en todos los 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	node1-01_clus1	true
Cluster	node1-01_clus2	true
Cluster	node1-02_clus1	true
Cluster	node1-02_clus2	true
Cluster	node1-03_clus1	true
Cluster	node1-03_clus2	true
Cluster	node1-04_clus1	true
Cluster	node1-04_clus2	true

8 entries were displayed.

El futuro

Una vez que se haya preparado para instalar el software NX-OS y RCF, debe [instalar o actualizar el software NX-OS](#) .

Instale o actualice el software NX-OS

Siga este procedimiento para instalar o actualizar el software NX-OS en el conmutador Nexus 9332D-GX2B.

Revise los requisitos

Antes de empezar

Verifique lo siguiente:

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

- ["Página del switch Cisco Ethernet"](#)

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

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

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

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

Proporciona información sobre actualización/degradación disruptiva para software Cisco NX-OS en los switches de la serie Nexus 9000 en función de tus versiones actuales y objetivo.

En la página, selecciona **Actualización disruptiva** y selecciona tu versión actual y la versión de destino de la lista desplegable.

Acerca de los ejemplos

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

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

Instale el software

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.



- NX-OS 10.4.2 es la única versión compatible con los conmutadores Cisco Nexus 9332D-GX2B en un clúster ONTAP .
- No actualice ni degrade su versión de NX-OS a una versión no compatible; actualmente solo se admite la versión 10.4.2.

Pasos

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

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

node1-01/cdp				
C9332D-GX2B	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B	.			
C9332D-GX2B	.			
C9332D-GX2B	.			
C9332D-GX2B	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B				
node1-01/lldp				
	e10a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/3	-
	e10b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/3	-
	e11a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/4	-
	e11b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/4	-
	e1a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/1	-
	e1b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/1	-
	.			
	.			
	.			
	e7a	cs1 (c8:60:8f:34:78:d3)	Ethernet1/16/2	-
	e7b	cs2 (04:e3:87:19:a2:59)	Ethernet1/16/2	-
	.			
	.			
	.			

4. Consulta el estado administrativo y operativo de cada puerto.

a. **Puertos de clúster**

i. 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: node1-01

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

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

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

8 entries were displayed.

iii. 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

cs2 (FDOXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
cs1 (FLMXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.253
Serial Number: FLMXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
2 entries were displayed.		

b. Puertos HA

- Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01  
(system ha interconnect status show)
```

```
Node: node1-01  
Link 0 Status: up  
Link 1 Status: up  
Is Link 0 Active: true  
Is Link 1 Active: true  
IC RDMA Connection: up  
Slot: 0  
Debug Firmware: no
```

```
Interconnect Port 0 :  
Port Name: e1a-17  
MTU: 4096  
Link Information: ACTIVE
```

```
Interconnect Port 1 :  
Port Name: e1b-18  
MTU: 4096  
Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02  
(system ha interconnect status show)
```

```
Node: node1-02  
Link 0 Status: up  
Link 1 Status: up  
Is Link 0 Active: true  
Is Link 1 Active: true  
IC RDMA Connection: up  
Slot: 0  
Debug Firmware: no
```

```
Interconnect Port 0 :  
Port Name: e1a-17  
MTU: 4096  
Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

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

6. Copie el software NX-OS y las imágenes EPLD al conmutador Nexus 9332D-GX2B.

Muestra el ejemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.10.4.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: root

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
root@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.10.4.2.bin /bootflash/nxos.10.4.2.bin
/code/nxos.10.4.2.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.10.4.2.F.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.10.4.2.F.img /bootflash/n9000-
epld.10.4.2.F.img
/code/n9000-epld.10.4.2.F.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. 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) 2002-2025, 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 01.14
```

```
NXOS: version 10.4(1) [Feature Release]
```

```
Host NXOS: version 10.4(1)
```

```
BIOS compile time: 11/25/2024
```

```
NXOS image file is: bootflash:///nxos64-cs.10.4.1.F.bin
```

```
NXOS compile time: 11/30/2023 12:00:00 [12/14/2023 05:25:50]
```

```
NXOS boot mode: LXC
```

Hardware

```
cisco Nexus9000 C9332D-GX2B Chassis
```

```
Intel(R) Xeon(R) CPU D-1633N @ 2.50GHz with 32802156 kB of memory.
```

```
Processor Board ID FLMXXXXXXXXX
```

```
Device name: cs2
```

```
bootflash: 115802886 kB
```

```
Kernel uptime is 5 day(s), 2 hour(s), 13 minute(s), 21 second(s)
```

```
Last reset at 3580 usecs after Thu Jun 5 15:55:08 2025
```

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

```
System version: 10.4(1)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

8. 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.10.4.2.bin
```

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

```
Verifying image bootflash:/nxos.10.4.2.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

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

```
Preparing "nxos" version info using image  
bootflash:/nxos.10.4.2.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image  
bootflash:/nxos.10.4.2.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	10.4 (1)	10.4 (2)
Yes			
1	bios	xx.xx.:xx.xx	xxx
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.

9. 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) 2002-2025, 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 01.14
```

```
NXOS: version 10.4(2) [Feature Release]
```

```
Host NXOS: version 10.4(2)
```

```
BIOS compile time: 11/25/2024
```

```
NXOS image file is: bootflash:///nxos64-cs.10.4.2.F.bin
```

```
NXOS compile time: 11/30/2023 12:00:00 [12/14/2023 05:25:50]
```

```
NXOS boot mode: LXC
```

Hardware

```
cisco Nexus9000 C9332D-GX2B Chassis
```

```
Intel(R) Xeon(R) CPU D-1633N @ 2.50GHz with 32802156 kB of memory.
```

```
Processor Board ID FLMXXXXXXXXX
```

```
Device name: cs2
```

```
bootflash: 115802886 kB
```



```
Kernel uptime is 5 day(s), 2 hour(s), 13 minute(s), 21 second(s)
```

```
Last reset at 3580 usecs after Thu Jun 5 15:55:08 2025
```

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

```
System version: 10.4(2)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

10. 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.10.4.2.F.img module all
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

11. Tras reiniciar el 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

12. Verificar el estado de todos los puertos del clúster.

a. Puertos de clúster

- i. 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: node1-01

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

ii. Compruebe el estado del switch del clúster:

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

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

Muestra el ejemplo

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

node1-02/cdp
      e10a  cs1 (FLMXXXXXXXXX)      Ethernet1/16/3
N9K-C9332D-GX2B
      e10b  cs2 (FDOXXXXXXXXX)      Ethernet1/16/3
N9K-C9332D-GX2B
      e11a  cs1 (FLMXXXXXXXXX)      Ethernet1/16/4
N9K-C9332D-GX2B
      e11b  cs2 (FDOXXXXXXXXX)      Ethernet1/16/4
N9K-C9332D-GX2B
      e1a   cs1 (FLMXXXXXXXXX)      Ethernet1/16/1
N9K-C9332D-GX2B
      e1b   cs2 (FDOXXXXXXXXX)      Ethernet1/16/1
N9K-C9332D-GX2B
      .
      .
      .
      e7a   cs1 (FLM284504N6)       Ethernet1/16/2
N9K-C9332D-GX2B
      e7b   cs2 (FDO2846056X)       Ethernet1/16/2
N9K-C9332D-GX2B

node1-01/cdp
      e10a  cs1 (FLMXXXXXXXXX)      Ethernet1/16/3
N9K-C9332D-GX2B
      e10b  cs2 (FDOXXXXXXXXX)      Ethernet1/16/3
N9K-C9332D-GX2B
      e11a  cs1 (FLMXXXXXXXXX)      Ethernet1/16/4
N9K-C9332D-GX2B
      e11b  cs2 (FDOXXXXXXXXX)      Ethernet1/16/4
N9K-C9332D-GX2B
      e1a   cs1 (FLMXXXXXXXXX)      Ethernet1/16/1
N9K-C9332D-GX2B
      e1b   cs2 (FDOXXXXXXXXX)      Ethernet1/16/1
N9K-C9332D-GX2B
      .
      .
      .
      e7a   cs1 (FLMXXXXXXXXX)      Ethernet1/16/2
N9K-C9332D-GX2B
      e7b   cs2 (FDOXXXXXXXXX)      Ethernet1/16/2
N9K-C9332D-GX2B
      .
```

```

.
.

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                Type                                Address
Model                                -----
-----
cs2 (FDOXXXXXXXXX)                   cluster-network                   10.228.137.233
N9K-C9332D-GX2B
    Serial Number: FDOXXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

cs1 (FLMXXXXXXXXX)                   cluster-network                   10.228.137.253
N9K-C9332D-GX2B
    Serial Number: FLMXXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

```

b. Puertos HA

- i. Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```


Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

```
16 entries were displayed.
```

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

13. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	false
node1-04	true	true	true

4 entries were displayed.

14. Repita los pasos 6 a 13 para instalar el software NX-OS y las imágenes EPLD en el conmutador cs1.
15. Habilite la reversión automática en las LIF del clúster.

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

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

Si alguna LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

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

El futuro

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

Instale o actualice el RCF

Instale o actualice la descripción general del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar el conmutador Nexus 9332D-GX2B por primera vez. Actualiza tu versión RCF cuando tienes una versión existente del archivo RCF instalado en tu conmutador.

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

Configuración RCF disponible

- **Cluster-HA-Storage:** admite tráfico compartido de clúster/HA/almacenamiento en puertos (NX9332D-GX2B-RCF-v10.0-Shared.txt).

Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

Documentación sugerida

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

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

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

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

Acerca de los ejemplos

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

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

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



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

Comandos utilizados

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.

El futuro

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

Instalación del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar el conmutador Nexus 9332D-GX2B por primera vez.

Antes de empezar

Compruebe las siguientes instalaciones y conexiones:

- Una conexión de consola al interruptor. La conexión de la consola es opcional si tiene acceso remoto al conmutador.
- El switch CS1 y el switch CS2 se encienden y la configuración inicial del switch se ha completado (la dirección IP de gestión y SSH está configurado).
- Se ha instalado la versión deseada de NX-OS.
- Las conexiones ISL entre los switches están conectadas.

Paso 1: Instale el RCF en los interruptores

1. Inicie sesión en el switch CS1 mediante SSH o mediante una consola de serie.
2. Copie el RCF al bootflash del switch CS1 usando 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 9000"](#) guías.

Muestra el ejemplo

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: NX9332D-GX2B-RCF-v10.0-Shared.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

3. Aplique el RCF descargado 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 9000"](#) guías.

Este ejemplo muestra el archivo RCF NX9332D-GX2B-RCF-v10.0-Shared.txt siendo instalado en el switch cs1:

```
cs1# copy NX9332D-GX2B-RCF-v10.0-Shared.txt running-config echo-commands
```

4. Examine el resultado del banner desde el `show banner motd` comando. Debe leer y seguir estas

instrucciones para asegurarse de que la configuración y el funcionamiento del interruptor son correctos.

Muestra el ejemplo

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : NX9332D-GX2B
* Filename    : NX9332D-GX2B-RCF-v10.0-Shared.txt
* Date       : 05-09-2025
* Version    : v10.0
* Port Usage:
* Ports 1-30: 100GbE Intra-Cluster/HA/Storage Ports, int e1/{1-
30}/1-4
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
*
* IMPORTANT NOTES
* Interface port-channel999 is reserved to identify the version of
this file.
*****
*****
```

5. 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.

6. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.

Asegúrese de configurar lo siguiente:



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

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

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

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

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

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

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

cs1# echo "hardware access-list tcam region ing-l2-qos 1536" >>
bootflash:write_erase.cfg
```

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

7. Verificar que el write_erase.cfg El archivo se completa como se esperaba:

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

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

```
cs1# write erase
```

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

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

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

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

10. Reinicie el switch:

```
cs1# reload
```

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

11. Repita los pasos 1 al 10 en el interruptor cs2.

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

Paso 2: Verifique las conexiones del interruptor

1. Verifique que los puertos del conmutador conectados a los puertos del clúster estén activos:

```
show interface brief
```

Muestra el ejemplo

```
cs1# show interface brief | grep up
.
.
Eth1/9/3          1      eth  trunk  up      none
100G(D) --
Eth1/9/4          1      eth  trunk  up      none
100G(D) --
Eth1/15/1         1      eth  trunk  up      none
100G(D) --
Eth1/15/2         1      eth  trunk  up      none
100G(D) --
Eth1/15/3         1      eth  trunk  up      none
100G(D) --
Eth1/15/4         1      eth  trunk  up      none
100G(D) --
Eth1/16/1         1      eth  trunk  up      none
100G(D) --
Eth1/16/2         1      eth  trunk  up      none
100G(D) --
Eth1/16/3         1      eth  trunk  up      none
100G(D) --
Eth1/16/4         1      eth  trunk  up      none
100G(D) --
Eth1/17/1         1      eth  trunk  up      none
100G(D) --
Eth1/17/2         1      eth  trunk  up      none
100G(D) --
Eth1/17/3         1      eth  trunk  up      none
100G(D) --
Eth1/17/4         1      eth  trunk  up      none
100G(D) --
.
.
```

2. Compruebe que los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Po1, Po999, Eth1/31, Eth1/32, Eth1/1/1, Eth1/1/2, Eth1/1/3, Eth1/1/4, Eth1/2/1, Eth1/2/2, Eth1/2/3, Eth1/2/4, Eth1/3/1, Eth1/3/2, Eth1/3/3, Eth1/3/4, Eth1/4/1, Eth1/4/2, Eth1/4/3, Eth1/4/4, Eth1/5/1, Eth1/5/2, Eth1/5/3, Eth1/5/4, Eth1/6/1, Eth1/6/2, Eth1/6/3, Eth1/6/4, Eth1/7/1, Eth1/7/2, Eth1/7/3, Eth1/7/4, Eth1/8/1, Eth1/8/2, Eth1/8/3, Eth1/8/4, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4, Eth1/11/1, Eth1/11/2, Eth1/11/3, Eth1/11/4, Eth1/12/1, Eth1/12/2, Eth1/12/3, Eth1/12/4, Eth1/13/1, Eth1/13/2, Eth1/13/3, Eth1/13/4, Eth1/14/1, Eth1/14/2, Eth1/14/3

Eth1/15/1, Eth1/15/2		Eth1/14/4,
Eth1/15/4, Eth1/16/1		Eth1/15/3,
Eth1/16/3, Eth1/16/4		Eth1/16/2,
Eth1/17/2, Eth1/17/3		Eth1/17/1,
Eth1/18/1, Eth1/18/2		Eth1/17/4,
Eth1/18/4, Eth1/19/1		Eth1/18/3,
Eth1/19/3, Eth1/19/4		Eth1/19/2,
Eth1/20/2, Eth1/20/3		Eth1/20/1,
Eth1/21/1, Eth1/21/2		Eth1/20/4,
Eth1/21/4, Eth1/22/1		Eth1/21/3,
Eth1/22/3, Eth1/22/4		Eth1/22/2,
Eth1/23/2, Eth1/23/3		Eth1/23/1,
Eth1/24/1, Eth1/24/2		Eth1/23/4,
Eth1/24/4, Eth1/25/1		Eth1/24/3,
Eth1/25/3, Eth1/25/4		Eth1/25/2,
Eth1/26/2, Eth1/26/3		Eth1/26/1,
Eth1/27/1, Eth1/27/2		Eth1/26/4,
Eth1/27/4, Eth1/28/1		Eth1/27/3,
Eth1/28/3, Eth1/28/4		Eth1/28/2,
Eth1/29/2, Eth1/29/3		Eth1/29/1,
Eth1/30/1, Eth1/30/2		Eth1/29/4,
17 VLAN0017	active	Eth1/30/3, Eth1/30/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
		Eth1/1/4, Eth1/2/1,

Eth1/2/2	Eth1/2/3, Eth1/2/4,
Eth1/3/1	Eth1/3/2, Eth1/3/3,
Eth1/3/4	Eth1/4/1, Eth1/4/2,
Eth1/4/3	Eth1/4/4, Eth1/5/1,
Eth1/5/2	Eth1/5/3, Eth1/5/4,
Eth1/6/1	Eth1/6/2, Eth1/6/3,
Eth1/6/4	Eth1/7/1, Eth1/7/2,
Eth1/7/3	Eth1/7/4, Eth1/8/1,
Eth1/8/2	Eth1/8/3, Eth1/8/4,
Eth1/9/1	Eth1/9/2, Eth1/9/3,
Eth1/9/4	Eth1/10/1,
Eth1/10/2, Eth1/10/3	Eth1/10/4,
Eth1/11/1, Eth1/11/2	Eth1/11/3,
Eth1/11/4, Eth1/12/1	Eth1/12/2,
Eth1/12/3, Eth1/12/4	Eth1/13/1,
Eth1/13/2, Eth1/13/3	Eth1/13/4,
Eth1/14/1, Eth1/14/2	Eth1/14/3,
Eth1/14/4, Eth1/15/1	Eth1/15/2,
Eth1/15/3, Eth1/15/4	Eth1/16/1,
Eth1/16/2, Eth1/16/3	Eth1/16/4,
Eth1/17/1, Eth1/17/2	Eth1/17/3,
Eth1/17/4, Eth1/18/1	Eth1/18/2,
Eth1/18/3, Eth1/18/4	Eth1/19/1,

Eth1/19/2, Eth1/19/3		Eth1/19/4,
Eth1/20/1, Eth1/20/2		Eth1/20/3,
Eth1/20/4, Eth1/21/1		Eth1/21/2,
Eth1/21/3, Eth1/21/4		Eth1/22/1,
Eth1/22/2, Eth1/22/3		Eth1/22/4,
Eth1/23/1, Eth1/23/2		Eth1/23/3,
Eth1/23/4, Eth1/24/1		Eth1/24/2,
Eth1/24/3, Eth1/24/4		Eth1/25/1,
Eth1/25/2, Eth1/25/3		Eth1/25/4,
Eth1/26/1, Eth1/26/2		Eth1/26/3,
Eth1/26/4, Eth1/27/1		Eth1/27/2,
Eth1/27/3, Eth1/27/4		Eth1/28/1,
Eth1/28/2, Eth1/28/3		Eth1/28/4,
Eth1/29/1, Eth1/29/2		Eth1/29/3,
Eth1/29/4, Eth1/30/1		Eth1/30/2,
Eth1/30/3, Eth1/30/4		
18 VLAN0018	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,

Eth1/6/4	Eth1/7/1, Eth1/7/2,
Eth1/7/3	Eth1/7/4, Eth1/8/1,
Eth1/8/2	Eth1/8/3, Eth1/8/4,
Eth1/9/1	Eth1/9/2, Eth1/9/3,
Eth1/9/4	Eth1/10/1,
Eth1/10/2, Eth1/10/3	Eth1/10/4,
Eth1/11/1, Eth1/11/2	Eth1/11/3,
Eth1/11/4, Eth1/12/1	Eth1/12/2,
Eth1/12/3, Eth1/12/4	Eth1/13/1,
Eth1/13/2, Eth1/13/3	Eth1/13/4,
Eth1/14/1, Eth1/14/2	Eth1/14/3,
Eth1/14/4, Eth1/15/1	Eth1/15/2,
Eth1/15/3, Eth1/15/4	Eth1/16/1,
Eth1/16/2, Eth1/16/3	Eth1/16/4,
Eth1/17/1, Eth1/17/2	Eth1/17/3,
Eth1/17/4, Eth1/18/1	Eth1/18/2,
Eth1/18/3, Eth1/18/4	Eth1/19/1,
Eth1/19/2, Eth1/19/3	Eth1/19/4,
Eth1/20/1, Eth1/20/2	Eth1/20/3,
Eth1/20/4, Eth1/21/1	Eth1/21/2,
Eth1/21/3, Eth1/21/4	Eth1/22/1,
Eth1/22/2, Eth1/22/3	Eth1/22/4,
Eth1/23/1, Eth1/23/2	Eth1/23/3,

Eth1/23/4, Eth1/24/1		Eth1/24/2,
Eth1/24/3, Eth1/24/4		Eth1/25/1,
Eth1/25/2, Eth1/25/3		Eth1/25/4,
Eth1/26/1, Eth1/26/2		Eth1/26/3,
Eth1/26/4, Eth1/27/1		Eth1/27/2,
Eth1/27/3, Eth1/27/4		Eth1/28/1,
Eth1/28/2, Eth1/28/3		Eth1/28/4,
Eth1/29/1, Eth1/29/2		Eth1/29/3,
Eth1/29/4, Eth1/30/1		Eth1/30/2,
Eth1/30/3, Eth1/30/4		
30 VLAN0030	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,
Eth1/6/4		Eth1/7/1, Eth1/7/2,
Eth1/7/3		Eth1/7/4, Eth1/8/1,
Eth1/8/2		Eth1/8/3, Eth1/8/4,
Eth1/9/1		Eth1/9/2, Eth1/9/3,
Eth1/9/4		Eth1/10/1,
Eth1/10/2, Eth1/10/3		Eth1/10/4,

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/2, Eth1/28/3		Eth1/28/4,
Eth1/29/1, Eth1/29/2		Eth1/29/3,
Eth1/29/4, Eth1/30/1		Eth1/30/2,
Eth1/30/3, Eth1/30/4		
40 VLAN0040	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,
Eth1/6/4		Eth1/7/1, Eth1/7/2,
Eth1/7/3		Eth1/7/4, Eth1/8/1,
Eth1/8/2		Eth1/8/3, Eth1/8/4,
Eth1/9/1		Eth1/9/2, Eth1/9/3,
Eth1/9/4		Eth1/10/1,
Eth1/10/2, Eth1/10/3		Eth1/10/4,
Eth1/11/1, Eth1/11/2		Eth1/11/3,
Eth1/11/4, Eth1/12/1		Eth1/12/2,
Eth1/12/3, Eth1/12/4		Eth1/13/1,
Eth1/13/2, Eth1/13/3		Eth1/13/4,
Eth1/14/1, Eth1/14/2		Eth1/14/3,
Eth1/14/4, Eth1/15/1		Eth1/15/2,

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

cs1# **show interface trunk**

```
-----  
-----  
Port          Native  Status      Port
```

	Vlan	Channel	

Eth1/1/1	1	trunking	--
Eth1/1/2	1	trunking	--
Eth1/1/3	1	trunking	--
Eth1/1/4	1	trunking	--
Eth1/2/1	1	trunking	--
Eth1/2/2	1	trunking	--
Eth1/2/3	1	trunking	--
Eth1/2/4	1	trunking	--
.			
.			
.			
Eth1/30/1	none		
Eth1/30/2	none		
Eth1/30/3	none		
Eth1/30/4	none		
Eth1/31	none		
Eth1/32	none		
Po1	1		



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

3. 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)
999    Po999 (SD)    Eth      NONE      --
cs1#
```

Paso 3: Configure el cluster ONTAP

NetApp recomienda usar System Manager para configurar clústeres nuevos.

System Manager proporciona un flujo de trabajo sencillo y sencillo para la instalación y la configuración del clúster, incluidas la asignación de una dirección IP de gestión de nodos, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento del almacenamiento inicial.

Vaya a ["Configure ONTAP en un nuevo clúster con System Manager"](#) para obtener instrucciones de configuración.

El futuro

Después de haber instalado el RCF, ["verificar la configuración de SSH"](#).

Actualice su archivo de configuración de referencia (RCF)

Actualice la versión de RCF cuando tenga instalada una versión existente del archivo RCF en los conmutadores operativos.

Antes de empezar

Asegúrese de tener lo siguiente:

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El RCF actual.

- Si está actualizando la versión de RCF, necesita una configuración de inicio en el RCF que refleje las imágenes de inicio deseadas.

Si necesita cambiar la configuración 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.



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.



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

Paso 1: Prepárese para la actualización

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.

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

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

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

```
network device-discovery show
```

Muestra el ejemplo

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

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

node1-01/cdp				
C9332D-GX2B	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B	.			
C9332D-GX2B	.			
C9332D-GX2B	.			
C9332D-GX2B	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2	N9K-
node1-01/lldp				
	e10a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/3	-
	e10b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/3	-
	e11a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/4	-
	e11b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/4	-
	e1a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/1	-
	e1b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/1	-
	.			
	.			
	.			
	e7a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/2	-
	e7b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/16/2	-

4. Consulta el estado administrativo y operativo de cada puerto.

a. **Puertos de clúster**

- i. 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: node1-01

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

ii. 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
```

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

Cluster			
	node1-01_clus1	up/up	169.254.3.4/23
node1-01	e7a true		
	node1-01_clus2	up/up	169.254.3.5/23
node1-01	e7b true		
	node1-02_clus1	up/up	169.254.3.8/23
node1-02	e7a true		
	node1-02_clus2	up/up	169.254.3.9/23
node1-02	e7b true		
	node1-03_clus1	up/up	169.254.1.3/23
node1-03	e7a true		
	node1-03_clus2	up/up	169.254.1.1/23
node1-03	e7b true		
	node1-04_clus1	up/up	169.254.1.6/23
node1-04	e7a true		
	node1-04_clus2	up/up	169.254.1.7/23
node1-04	e7b true		
8 entries were displayed.			

iii. Verifique que el clúster muestre información para ambos conmutadores:

```
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

cs2 (FDOXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
cs2 (FLMXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.234
Serial Number: FLMXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
2 entries were displayed.		

b. Puertos HA

- Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

Node	Port	Type	Mode	Speed (Gb/s)	State	Status
-----	----	-----	-----	-----	-----	-----
node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf ID	Module	State	Internal?
1.1			
0	A	connected	false
1	A	connected	false
2	A	connected	false
3	A	connected	false
4	A	connected	false
5	A	connected	false
6	A	connected	false
7	A	connected	false
8	B	connected	false
9	B	connected	false
10	B	connected	false
11	B	connected	false
12	B	connected	false
13	B	connected	false
14	B	connected	false
15	B	connected	false

```
16 entries were displayed.
```

- ii. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

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


Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

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

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

Paso 2: Configurar puertos

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

```

cs1# config
cs1(config)# interface e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7/1-4,e1/8/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/9/1-4,e1/10/1-4,e1/11/1-4,e1/12/1-4,e1/13/1-4,e1/14/1-4,e1/15/1-4,e1/16/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/17/1-4,e1/18/1-4,e1/19/1-4,e1/20/1-4,e1/21/1-4,e1/22/1-44,e1/23/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/24/1-,e1/25/1-4,e1/26/1-4,e1/27/1-4,e1/28/1-4,e1/29/1-4,e1/30/1-44
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit

```



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

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

```

network interface show -role cluster

```

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

8 entries were displayed.

3. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

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

4 entries were displayed.
```

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

```
show running-config
```

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



Asegúrese de configurar lo siguiente:

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

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

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

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

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

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

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

```
cs1# echo "hardware access-list tcam region ing-l2-qos 1536" >>
```

```
bootflash:write_erase.cfg
```

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

6. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

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

7. Emitir el `write erase` Comando para borrar la configuración guardada actual:

```
cs1# write erase
```

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

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

8. Copie la configuración básica guardada anteriormente en la configuración de inicio.

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

9. Reinicie el switch:

```
cs1# reload
```

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

10. Cuando se pueda volver a acceder a la dirección IP de administración, inicie sesión en el switch a través de SSH.

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

11. Copie el RCF al bootflash del switch CS1 usando 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 9000"](#) guías.

Muestra el ejemplo

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: NX9332D-GX2B-RCF-v10.0-Shared.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)...
```

12. 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 9000"](#) guías.

Este ejemplo muestra el archivo RCF NX9332D-GX2B-RCF-v10.0-Shared.txt siendo instalado en el switch cs1:

```
cs1# copy NX9332D-GX2B-RCF-v10.0-Shared.txt running-config echo-commands
```



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

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

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

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

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

16. Reinicie el interruptor CS1. Puede ignorar las alertas de «monitor de estado del switch del clúster» y los eventos de «puertos inactivos» que se notifican en los nodos mientras se reinicia el switch.

```
cs1# reload
```

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

17. Verificar el estado de todos los puertos del clúster.

a. **Puertos de clúster**

- i. Compruebe que los puertos del clúster estén en buen estado en todos los nodos del clúster:

```
network port show -ip space cluster
```

Muestra el ejemplo

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

Node: node1

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

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

e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

ii. Compruebe el estado del switch del clúster.

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

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

Muestra el ejemplo

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

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

node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			

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

Switch Model	Type	Address

cs2 (FDOXXXXXXXXX) N9K-C9332D-GX2B	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4 (2)		

```
Version Source: CDP/ISDP
```

```
cs1 (FLMXXXXXXXX)          cluster-network    10.228.137.234  
N9K-C9332D-GX2B
```

```
Serial Number: FLMXXXXXXXX
```

```
Is Monitored: true
```

```
Reason: None
```

```
Software Version: Cisco Nexus Operating System (NX-OS)
```

```
Software, Version
```

```
10.4(2)
```

```
Version Source: CDP/ISDP
```

```
2 entries were displayed.
```

b. Puertos HA

- i. Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

                Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
    Is Link 0 Active: true
    Is Link 1 Active: true
    IC RDMA Connection: up
                Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
                Port Name: ela-17
                MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
                Port Name: elb-18
                MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

                Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
    Is Link 0 Active: true
    Is Link 1 Active: true
    IC RDMA Connection: up
                Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
                Port Name: ela-17
                MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
```

```
.
```

```
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

```
16 entries were displayed.
```

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

18. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

19. Repita los pasos 4 a 18 en el interruptor cs2.

20. Habilite la reversión automática en las LIF del clúster.

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

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

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
show interface brief
```


Muestra el ejemplo

```
cs1# show interface brief | grep up
.
.
Eth1/9/3      1      eth  trunk  up      none
100G(D)  --
Eth1/9/4      1      eth  trunk  up      none
100G(D)  --
Eth1/15/1     1      eth  trunk  up      none
100G(D)  --
Eth1/15/2     1      eth  trunk  up      none
100G(D)  --
Eth1/15/3     1      eth  trunk  up      none
100G(D)  --
Eth1/15/4     1      eth  trunk  up      none
100G(D)  --
Eth1/16/1     1      eth  trunk  up      none
100G(D)  --
Eth1/16/2     1      eth  trunk  up      none
100G(D)  --
Eth1/16/3     1      eth  trunk  up      none
100G(D)  --
Eth1/16/4     1      eth  trunk  up      none
100G(D)  --
Eth1/17/1     1      eth  trunk  up      none
100G(D)  --
Eth1/17/2     1      eth  trunk  up      none
100G(D)  --
Eth1/17/3     1      eth  trunk  up      none
100G(D)  --
Eth1/17/4     1      eth  trunk  up      none
100G(D)  --
.
.
.
```

2. Compruebe que los nodos esperados siguen conectados:

```
show cdp neighbors
```

Muestra el ejemplo

```
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
cs2 (FDOXXXXXXXXX) Eth1/63	Eth1/31	179	R S I s	N9K-C9364D-GX2A
cs2 (FDOXXXXXXXXX) Eth1/64	Eth1/32	179	R S I s	N9K-C9364D-GX2A
node1-01 e1a	Eth1/4/1	123	H	AFX-1K
node1-01 e7a	Eth1/4/2	123	H	AFX-1K
node1-01 e10a	Eth1/4/3	123	H	AFX-1K
node1-01 e11a	Eth1/4/4	123	H	AFX-1K
node1-02 e1a	Eth1/9/1	138	H	AFX-1K
node1-02 e7a	Eth1/9/2	138	H	AFX-1K
node1-02 e10a	Eth1/9/3	138	H	AFX-1K
node1-02 e11a	Eth1/9/4	138	H	AFX-1K
node1-03 e1a	Eth1/15/1	138	H	AFX-1K
node1-03 e7a	Eth1/15/2	138	H	AFX-1K
node1-03 e10a	Eth1/15/3	138	H	AFX-1K
node1-03 e11a	Eth1/15/4	138	H	AFX-1K
node1-04 e1a	Eth1/16/1	173	H	AFX-1K
node1-04 e7a	Eth1/16/2	173	H	AFX-1K
node1-04 e10a	Eth1/16/3	173	H	AFX-1K
node1-04	Eth1/16/4	173	H	AFX-1K

```
e11a
```

```
Total entries displayed: 18
```

3. Compruebe que los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Po999, Eth1/31, Eth1/32 Eth1/33, Eth1/34, Eth1/1/1 Eth1/1/2, Eth1/1/3, Eth1/1/4 Eth1/2/1, Eth1/2/2, Eth1/2/3 Eth1/2/4, Eth1/3/1, Eth1/3/2 Eth1/3/3, Eth1/3/4, Eth1/4/1 Eth1/4/2, Eth1/4/3, Eth1/4/4 Eth1/5/1, Eth1/5/2, Eth1/5/3 Eth1/5/4, Eth1/6/1, Eth1/6/2 Eth1/6/3, Eth1/6/4, Eth1/7/1 Eth1/7/2, Eth1/7/3, Eth1/7/4 Eth1/8/1, Eth1/8/2, Eth1/8/3 Eth1/8/4, Eth1/9/1, Eth1/9/2 Eth1/9/3, Eth1/9/4, Eth1/10/1 Eth1/10/2, Eth1/10/3, Eth1/10/4 Eth1/11/1, Eth1/11/2, Eth1/11/3 Eth1/11/4, Eth1/12/1, Eth1/12/2 Eth1/12/3, Eth1/12/4, Eth1/13/1 Eth1/13/2, Eth1/13/3, Eth1/13/4 Eth1/14/1,

Eth1/14/2, Eth1/14/3		Eth1/14/4,
Eth1/15/1, Eth1/15/2		Eth1/15/3,
Eth1/15/4, Eth1/16/1		Eth1/16/2,
Eth1/16/3, Eth1/16/4		Eth1/17/1,
Eth1/17/2, Eth1/17/3		Eth1/17/4,
Eth1/18/1, Eth1/18/2		Eth1/18/3,
Eth1/18/4, Eth1/19/1		Eth1/19/2,
Eth1/19/3, Eth1/19/4		Eth1/20/1,
Eth1/20/2, Eth1/20/3		Eth1/20/4,
Eth1/21/1, Eth1/21/2		Eth1/21/3,
Eth1/21/4, Eth1/22/1		Eth1/22/2,
Eth1/22/3, Eth1/22/4		Eth1/23/1,
Eth1/23/2, Eth1/23/3		Eth1/23/4,
Eth1/24/1, Eth1/24/2		Eth1/24/3,
Eth1/24/4, Eth1/25/1		Eth1/25/2,
Eth1/25/3, Eth1/25/4		Eth1/26/1,
Eth1/26/2, Eth1/26/3		Eth1/26/4,
Eth1/27/1, Eth1/27/2		Eth1/27/3,
Eth1/27/4, Eth1/28/1		Eth1/28/2,
Eth1/28/3, Eth1/28/4		Eth1/29/1,
Eth1/29/2, Eth1/29/3		Eth1/29/4,
Eth1/30/1, Eth1/30/2		Eth1/30/3, Eth1/30/4
17 VLAN0017	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		

Eth1/2/2	Eth1/1/4, Eth1/2/1,
Eth1/3/1	Eth1/2/3, Eth1/2/4,
Eth1/3/4	Eth1/3/2, Eth1/3/3,
Eth1/4/3	Eth1/4/1, Eth1/4/2,
Eth1/5/2	Eth1/4/4, Eth1/5/1,
Eth1/6/1	Eth1/5/3, Eth1/5/4,
Eth1/6/4	Eth1/6/2, Eth1/6/3,
Eth1/7/3	Eth1/7/1, Eth1/7/2,
Eth1/8/2	Eth1/7/4, Eth1/8/1,
Eth1/9/1	Eth1/8/3, Eth1/8/4,
Eth1/9/4	Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3	Eth1/10/1,
Eth1/11/1, Eth1/11/2	Eth1/10/4,
Eth1/11/4, Eth1/12/1	Eth1/11/3,
Eth1/12/3, Eth1/12/4	Eth1/12/2,
Eth1/13/2, Eth1/13/3	Eth1/13/1,
Eth1/14/1, Eth1/14/2	Eth1/13/4,
Eth1/14/4, Eth1/15/1	Eth1/14/3,
Eth1/15/3, Eth1/15/4	Eth1/15/2,
Eth1/16/2, Eth1/16/3	Eth1/16/1,
Eth1/17/1, Eth1/17/2	Eth1/16/4,
Eth1/17/4, Eth1/18/1	Eth1/17/3,
Eth1/18/3, Eth1/18/4	Eth1/18/2,

Eth1/19/2, Eth1/19/3		Eth1/19/1,
Eth1/20/1, Eth1/20/2		Eth1/19/4,
Eth1/20/4, Eth1/21/1		Eth1/20/3,
Eth1/21/3, Eth1/21/4		Eth1/21/2,
Eth1/22/2, Eth1/22/3		Eth1/22/1,
Eth1/23/1, Eth1/23/2		Eth1/22/4,
Eth1/23/4, Eth1/24/1		Eth1/23/3,
Eth1/24/3, Eth1/24/4		Eth1/24/2,
Eth1/25/2, Eth1/25/3		Eth1/25/1,
Eth1/26/1, Eth1/26/2		Eth1/25/4,
Eth1/26/4, Eth1/27/1		Eth1/26/3,
Eth1/27/3, Eth1/27/4		Eth1/27/2,
Eth1/28/2, Eth1/28/3		Eth1/28/1,
Eth1/29/1, Eth1/29/2		Eth1/28/4,
Eth1/29/4, Eth1/30/1		Eth1/29/3,
Eth1/30/3, Eth1/30/4		Eth1/30/2,
18 VLAN0018	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		

Eth1/6/4

Eth1/7/3

Eth1/8/2

Eth1/9/1

Eth1/9/4

Eth1/10/2, Eth1/10/3

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/6/2, Eth1/6/3,

Eth1/7/1, Eth1/7/2,

Eth1/7/4, Eth1/8/1,

Eth1/8/3, Eth1/8/4,

Eth1/9/2, Eth1/9/3,

Eth1/10/1,

Eth1/10/4,

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/4, Eth1/24/1		Eth1/23/3,
Eth1/24/3, Eth1/24/4		Eth1/24/2,
Eth1/25/2, Eth1/25/3		Eth1/25/1,
Eth1/26/1, Eth1/26/2		Eth1/25/4,
Eth1/26/4, Eth1/27/1		Eth1/26/3,
Eth1/27/3, Eth1/27/4		Eth1/27/2,
Eth1/28/2, Eth1/28/3		Eth1/28/1,
Eth1/29/1, Eth1/29/2		Eth1/28/4,
Eth1/29/4, Eth1/30/1		Eth1/29/3,
Eth1/30/3, Eth1/30/4		Eth1/30/2,
30 VLAN0030	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,
Eth1/6/4		Eth1/7/1, Eth1/7/2,
Eth1/7/3		Eth1/7/4, Eth1/8/1,
Eth1/8/2		Eth1/8/3, Eth1/8/4,
Eth1/9/1		Eth1/9/2, Eth1/9/3,
Eth1/9/4		Eth1/10/1,
Eth1/10/2, Eth1/10/3		

Eth1/11/1, Eth1/11/2
Eth1/11/4, Eth1/12/1
Eth1/12/3, Eth1/12/4
Eth1/13/2, Eth1/13/3
Eth1/14/1, Eth1/14/2
Eth1/14/4, Eth1/15/1
Eth1/15/3, Eth1/15/4
Eth1/16/2, Eth1/16/3
Eth1/17/1, Eth1/17/2
Eth1/17/4, Eth1/18/1
Eth1/18/3, Eth1/18/4
Eth1/19/2, Eth1/19/3
Eth1/20/1, Eth1/20/2
Eth1/20/4, Eth1/21/1
Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4

Eth1/10/4,
Eth1/11/3,
Eth1/12/2,
Eth1/13/1,
Eth1/13/4,
Eth1/14/3,
Eth1/15/2,
Eth1/16/1,
Eth1/16/4,
Eth1/17/3,
Eth1/18/2,
Eth1/19/1,
Eth1/19/4,
Eth1/20/3,
Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,

Eth1/28/2, Eth1/28/3		Eth1/28/1,
Eth1/29/1, Eth1/29/2		Eth1/28/4,
Eth1/29/4, Eth1/30/1		Eth1/29/3,
Eth1/30/3, Eth1/30/4		Eth1/30/2,
40 VLAN0040	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		Eth1/4/1, Eth1/4/2,
Eth1/4/3		Eth1/4/4, Eth1/5/1,
Eth1/5/2		Eth1/5/3, Eth1/5/4,
Eth1/6/1		Eth1/6/2, Eth1/6/3,
Eth1/6/4		Eth1/7/1, Eth1/7/2,
Eth1/7/3		Eth1/7/4, Eth1/8/1,
Eth1/8/2		Eth1/8/3, Eth1/8/4,
Eth1/9/1		Eth1/9/2, Eth1/9/3,
Eth1/9/4		Eth1/10/1,
Eth1/10/2, Eth1/10/3		Eth1/10/4,
Eth1/11/1, Eth1/11/2		Eth1/11/3,
Eth1/11/4, Eth1/12/1		Eth1/12/2,
Eth1/12/3, Eth1/12/4		Eth1/13/1,
Eth1/13/2, Eth1/13/3		Eth1/13/4,
Eth1/14/1, Eth1/14/2		Eth1/14/3,
Eth1/14/4, Eth1/15/1		

Eth1/15/3, Eth1/15/4
Eth1/16/2, Eth1/16/3
Eth1/17/1, Eth1/17/2
Eth1/17/4, Eth1/18/1
Eth1/18/3, Eth1/18/4
Eth1/19/2, Eth1/19/3
Eth1/20/1, Eth1/20/2
Eth1/20/4, Eth1/21/1
Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4

Eth1/15/2,
Eth1/16/1,
Eth1/16/4,
Eth1/17/3,
Eth1/18/2,
Eth1/19/1,
Eth1/19/4,
Eth1/20/3,
Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,

cs1# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1/1	1	trunking	--
Eth1/1/2	1	trunking	--
Eth1/1/3	1	trunking	--
Eth1/1/4	1	trunking	--
Eth1/2/1	1	trunking	--
Eth1/2/2	1	trunking	--
Eth1/2/3	1	trunking	--
Eth1/2/4	1	trunking	--
.			
.			
.			
Eth1/30/1	none		
Eth1/30/2	none		
Eth1/30/3	none		
Eth1/30/4	none		
Eth1/31	none		
Eth1/32	none		
Po1	1		



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

4. 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)
999    Po999 (SD)    Eth      NONE      --
cs1#
```

5. 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				
	node1-01_clus1	up/up	169.254.36.44/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.7.5/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.197.206/16	node1-02
e7a	true			
	node1-02_clus2	up/up	169.254.195.186/16	node1-02
e7b	true			
	node1-03_clus1	up/up	169.254.192.49/16	node1-03
e7a	true			
	node1-03_clus2	up/up	169.254.182.76/16	node1-03
e7b	true			
	node1-04_clus1	up/up	169.254.59.49/16	node1-04
e7a	true			
	node1-04_clus2	up/up	169.254.62.244/16	node1-04
e7b	true			

```
8 entries were displayed.
```

Si alguna LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

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

6. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

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

- Puedes utilizar el `network interface check cluster-connectivity show` Comando para mostrar los detalles de una verificación de accesibilidad para la conectividad del clúster:

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


Muestra el ejemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-02_clus1
none			
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-02_clus1
none			
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-01_clus1
none			
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-01_clus2
none			
.			
.			
.			

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

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node1-04
Getting addresses from network interface table...
Cluster node1-01_clus1 169.254.36.44 node1-01 e7a
Cluster node1-01_clus2 169.254.7.5 node1-01 e7b
Cluster node1-02_clus1 169.254.197.206 node1-02 e7a
Cluster node1-02_clus2 169.254.195.186 node1-02 e7b
Cluster node1-03_clus1 169.254.192.49 node1-03 e7a
Cluster node1-03_clus2 169.254.182.76 node1-03 e7b
Cluster node1-04_clus1 169.254.59.49 node1-04 e7a
Cluster node1-04_clus2 169.254.62.244 node1-04 e7b
Local = 169.254.59.49 169.254.62.244
Remote = 169.254.36.44 169.254.7.5 169.254.197.206 169.254.195.186
169.254.192.49 169.254.182.76
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 169.254.59.49 to Remote 169.254.182.76
    Local 169.254.59.49 to Remote 169.254.192.49
    Local 169.254.59.49 to Remote 169.254.195.186
    Local 169.254.59.49 to Remote 169.254.197.206
    Local 169.254.59.49 to Remote 169.254.36.44
    Local 169.254.59.49 to Remote 169.254.7.5
    Local 169.254.62.244 to Remote 169.254.182.76
    Local 169.254.62.244 to Remote 169.254.192.49
    Local 169.254.62.244 to Remote 169.254.195.186
    Local 169.254.62.244 to Remote 169.254.197.206
    Local 169.254.62.244 to Remote 169.254.36.44
    Local 169.254.62.244 to Remote 169.254.7.5
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

El futuro

Después de haber actualizado su RCF, ["verificar la configuración de SSH"](#) .

Compruebe su configuración SSH

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

Pasos

1. Compruebe que SSH está habilitado:

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

2. Compruebe que las claves SSH estén habilitadas:

```
show ssh key
```

Muestra el ejemplo

```
(switch)# show ssh key
```

```
rsa Keys generated:Wed May 14 18:49:37 2025
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQGCndfdJesautdCwk5Mk/7pKOF10IeShc9uBtj74  
F52vbjyflFHOCXX7Xf3Vopxs6L1hbgzCpFLo9E7pZBd3I+1AoLyQUltR3svzNieGY8ml  
WZGLtpKf/P2fDCd8JVJaejrwQhm49WUPiC6ziEqBDMOGhJpD2e9++umyDdr6  
NbmK8Q==
```

```
bitcount:1024
```

```
fingerprint:
```

```
SHA256:QtNU+Qq2I4ZfYwEfMEB1+z8w7xaKTlantTdsjLBx+OU
```

```
could not retrieve dsa key information
```

```
ecdsa Keys generated:Wed May 14 18:50:56 2025
```

```
ecdsa-sha2-nistp521
```

```
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBAAAYnv17T+JlGmH8  
rg81xiOow0mPmkbkIG0o7h9EchixO3i3KjgQr8AwqkRHNTcQC3lRnizhJFUeMGCwuQTu  
rziRCwE6fAOkWa2MRyXA1DYRKXjVEOnW9+MvinMipHQ0cCc  
YSExhh7j4HvWHIuYv8RmD7e3rmDQFlyyiLwdmpGfas2yaw==
```

```
bitcount:521
```

```
fingerprint:
```

```
SHA256:7cpZ5NGnIq5Iamw67ke+9o4qG9D3xxmGPauV14X5934
```

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

El futuro

Después de haber verificado su configuración SSH, ["configurar la monitorización del estado del conmutador"](#) .

Restablecer el interruptor 9332D-GX2B a los valores predeterminados de fábrica

Para restablecer el interruptor 9332D-GX2B a los valores predeterminados de fábrica, debe borrar la configuración del interruptor 9332D-GX2B.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Borrar la configuración existente:

```
write erase
```

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

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

2. Recargue el software del conmutador:

```
reload
```

```
(cs2)# reload
```

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

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

Reemplazar un conmutador Cisco Nexus 9332D-GX2B

Siga estos pasos para reemplazar un conmutador Nexus 9332D-GX2B defectuoso en una red compartida. Este es un procedimiento no disruptivo (NDU).

Revise los requisitos

Antes de realizar la sustitución del interruptor, asegúrese de que:

- Ha verificado el número de serie del interruptor para asegurarse de que se sustituye el interruptor correcto.
- 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 ONTAP `cluster ping-cluster -node <node-name>` El comando debe indicar que la conectividad básica y la comunicación mayor que PMTU son exitosas en todas las rutas.
- En el interruptor de reemplazo Nexus 9332D-GX2B:
 - 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 1/30.
 - Todos los puertos de enlace entre conmutadores (ISL) están deshabilitados en los puertos 1/31 y 1/32.
 - El archivo de configuración de referencia (RCF) y el conmutador de imagen del sistema operativo NX-OS se cargan en el conmutador.
 - La personalización inicial del conmutador está completa, como se detalla en ["Configurar el conmutador de clúster 9332D-GX2B"](#).

Cualquier personalización de sitio anterior, como STP, SNMP y SSH, se copian al nuevo switch.

- Ha ejecutado el comando para migrar una LIF de clúster desde el nodo en el que se aloja la LIF del clúster.

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después de las tareas de mantenimiento para deshabilitar la creación de casos durante el mantenimiento. Consulte este artículo de la base de conocimientos ["SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#) para obtener más detalles.
- Habilite el registro de sesiones para cualquier sesión de CLI. Para obtener instrucciones sobre cómo activar el registro de sesiones, consulte la sección «Salida de sesión de registro» de este artículo de la base de conocimientos ["Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP"](#).

Sustituya el interruptor

Acerca de los ejemplos

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

- Los nombres de los conmutadores Nexus 9332D-GX2B existentes son cs1 y cs2.
- El nombre del nuevo conmutador Nexus 9332D-GX2B es newcs2.
- Los nombres de los nodos son node1-01, node1-02, node1-03 y node1-04.
- Los nombres de clúster LIF son node1-01_clus1 y node1-01_clus2 para el nodo1-01, node1-02_clus1 y node1-02_clus2 para el nodo1-02, node1-03_clus1 y node1-03_clus2 para el nodo1-03, y node1-04_clus1 y node1-04_clus2 para el nodo1-04.
- El símbolo del sistema de cambios en todos los nodos del cluster es cluster1:*>

Acerca de esta tarea

El siguiente procedimiento se basa en la siguiente topología de red de clúster:

Muestra el ejemplo

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

Node: node1-01

Ignore

						Speed(Mbps)	Health
Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	-----	-----	-----
-----	e7a	Cluster	Cluster	up	9000	auto/100000	healthy
false	e7b	Cluster	Cluster	up	9000	auto/100000	healthy
false							

Node: node1-02

Ignore

						Speed(Mbps)	Health
Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	-----	-----	-----
-----	e7a	Cluster	Cluster	up	9000	auto/100000	healthy
false	e7b	Cluster	Cluster	up	9000	auto/100000	healthy
false							

Node: node1-03

Ignore

						Speed(Mbps)	Health
Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	-----	-----	-----
-----	e7a	Cluster	Cluster	up	9000	auto/100000	healthy
false	e7b	Cluster	Cluster	up	9000	auto/100000	healthy

false

Node: node1-04

Ignore

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

e7a	Cluster	Cluster		up	9000	auto/100000	healthy
false							
e7b	Cluster	Cluster		up	9000	auto/100000	healthy
false							

8 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					
	node1-01_clus1	up/up	169.254.36.44/16	node1-01	e7a
true					
	node1-01_clus2	up/up	169.254.7.5/16	node1-01	e7b
true					
	node1-02_clus1	up/up	169.254.197.206/16	node1-02	e7a
true					
	node1-02_clus2	up/up	169.254.195.186/16	node1-02	e7b
true					
	node1-03_clus1	up/up	169.254.192.49/16	node1-03	e7a
true					
	node1-03_clus2	up/up	169.254.182.76/16	node1-03	e7b
true					
	node1-04_clus1	up/up	169.254.59.49/16	node1-04	e7a
true					
	node1-04_clus2	up/up	169.254.62.244/16	node1-04	e7b
true					

8 entries were displayed.


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

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

node1-01/cdp				
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B				
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3	N9K-
C9332D-GX2B				
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B				
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4	N9K-
C9332D-GX2B				
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B				
	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1	N9K-
C9332D-GX2B				
	.			
	.			
	.			
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B				
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2	N9K-
C9332D-GX2B				

```
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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
Device-ID Port ID					
cs2 (FDOXXXXXXXXX)	Eth1/31	179	R S I s	N9K-C9364D-GX2A	
Eth1/63					
cs2 (FDOXXXXXXXXX)	Eth1/32	179	R S I s	N9K-C9364D-GX2A	
Eth1/64					
node1-01	Eth1/4/1	123	H	AFX-1K	
e1a					
node1-01	Eth1/4/2	123	H	AFX-1K	
e7a					

node1-01	Eth1/4/3	123	H	AFX-1K
e10a				
node1-01	Eth1/4/4	123	H	AFX-1K
e11a				
node1-02	Eth1/9/1	138	H	AFX-1K
e1a				
node1-02	Eth1/9/2	138	H	AFX-1K
e7a				
node1-02	Eth1/9/3	138	H	AFX-1K
e10a				
node1-02	Eth1/9/4	138	H	AFX-1K
e11a				
node1-03	Eth1/15/1	138	H	AFX-1K
e1a				
node1-03	Eth1/15/2	138	H	AFX-1K
e7a				
node1-03	Eth1/15/3	138	H	AFX-1K
e10a				
node1-03	Eth1/15/4	138	H	AFX-1K
e11a				
node1-04	Eth1/16/1	173	H	AFX-1K
e1a				
node1-04	Eth1/16/2	173	H	AFX-1K
e7a				
node1-04	Eth1/16/3	173	H	AFX-1K
e10a				
node1-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

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					
Device-ID	Local Intrfce	Hldtme	Capability	Platform	
Port ID					
cs1 (FLMXXXXXXXX)	Eth1/31	179	R S I s	N9K-C9364D-GX2A	
Eth1/63					
cs1 (FLMXXXXXXXX)	Eth1/32	179	R S I s	N9K-C9364D-GX2A	
Eth1/64					

node1-01	Eth1/4/1	123	H	AFX-1K
e1a				
node1-01	Eth1/4/2	123	H	AFX-1K
e7a				
node1-01	Eth1/4/3	123	H	AFX-1K
e10a				
node1-01	Eth1/4/4	123	H	AFX-1K
e11a				
node1-02	Eth1/9/1	138	H	AFX-1K
e1a				
node1-02	Eth1/9/2	138	H	AFX-1K
e7a				
node1-02	Eth1/9/3	138	H	AFX-1K
e10a				
node1-02	Eth1/9/4	138	H	AFX-1K
e11a				
node1-03	Eth1/15/1	138	H	AFX-1K
e1a				
node1-03	Eth1/15/2	138	H	AFX-1K
e7a				
node1-03	Eth1/15/3	138	H	AFX-1K
e10a				
node1-03	Eth1/15/4	138	H	AFX-1K
e11a				
node1-04	Eth1/16/1	173	H	AFX-1K
e1a				
node1-04	Eth1/16/2	173	H	AFX-1K
e7a				
node1-04	Eth1/16/3	173	H	AFX-1K
e10a				
node1-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

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
```

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. 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 Descarga.
 - 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.
3. En el nuevo conmutador, inicie sesión como administrador y apague todos los puertos que estarán conectados a las interfaces del clúster de nodos (puertos 1/1 a 1/30).

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
newcs2(config)# interface e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7/1-4,e1/8/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/9/1-4,e1/10/1-4,e1/11/1-4,e1/12/1-4,e1/13/1-4,e1/14/1-4,e1/15/1-4,e1/16/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/17/1-4,e1/18/1-4,e1/19/1-4,e1/20/1-4,e1/21/1-4,e1/22/1-44,e1/23/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/24/1-,e1/25/1-4,e1/26/1-4,e1/27/1-4,e1/28/1-4,e1/29/1-4,e1/30/1-44
newcs2(config-if-range)# shutdown
newcs2(config-if-range)# exit
newcs2(config)# exit
```

4. 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	node1-01_clus1	true
Cluster	node1-02_clus2	true
Cluster	node1-03_clus1	true
Cluster	node1-04_clus2	true

4 entries were displayed.

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

- Puedes utilizar el `network interface check cluster-connectivity show` Comando para mostrar los detalles de una verificación de accesibilidad para la conectividad del clúster:

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

Muestra el ejemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-
02_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-
02_clus2	none		
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-
01_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-
01_clus2	none		
.			
.			
.			

- b. Alternativamente, también puedes utilizar el `cluster ping-cluster -node <node-name>` Comando para comprobar la conectividad:

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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 Eth1/31 y Eth1/32 en el conmutador Nexus 9332D-GX2B cs1.

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/31-32
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit
```

2. Retire todos los cables del conmutador Nexus 9332D-GX2B cs2 y luego conéctelos a los mismos puertos en el conmutador newcs2 9332D-GX2B.
3. Active los puertos ISL Eth1/31 y Eth1/32 entre los conmutadores cs1 y newcs2 y luego verifique el estado de funcionamiento del canal del puerto.

El canal del puerto debe indicar Po1(SU) y los puertos miembros deben indicar Eth1/31(P) y Eth1/32(P).

Muestra el ejemplo

Este ejemplo habilita los puertos ISL Eth1/31 y Eth1/32 y muestra el resumen del canal del puerto en el conmutador cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/31-32
cs1(config-if-range)# no shutdown
cs1(config-if-range)# exit
cs1(config)# exit
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      Eth1/31 (P)  Eth1/32 (P)
999    Po999 (SD)    Eth      NONE      --
```

4. Verifique que el puerto e7b 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: node1-01

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-02

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-03

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	

```

healthy false
e7b          Cluster      Cluster      up    9000  auto/100000
healthy false

Node: node1-04

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e7a        Cluster      Cluster      up    9000  auto/100000
healthy false
e7b        Cluster      Cluster      up    9000  auto/100000
healthy false

8 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, el nodo LIF node1-01_clus2 en el nodo1-01 se revierte exitosamente si el valor de Inicio es verdadero y el puerto es e7b.

Los siguientes comandos devuelven LIF node1-01_clus2 en node1-01 al puerto base e7a y muestra información sobre los LIF en ambos nodos. La activación del primer nodo se realiza correctamente si la columna Is Home es verdadera para ambas interfaces del clúster y muestran las asignaciones de puerto correctas, en este ejemplo e7a y e7b en el nodo1-01.

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

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

Cluster				
	node1-01_clus1	up/up	169.254.209.69/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.49.125/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.47.194/16	node1-02
e7b	true			
	node1-02_clus2	up/up	169.254.19.183/16	node1-02
e7a	false			
	.			
	.			
	.			

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
-----	-----	-----
node1-01	false	true
node1-02	true	true
node1-03	true	true
node1-04	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: node1-01

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-02

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

.
. .
. .

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

- Puedes utilizar el `network interface check cluster-connectivity` Comando para mostrar los detalles de una verificación de accesibilidad para la conectividad del clúster:

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

Muestra el ejemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-
02_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-
02_clus2	none		
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-
01_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-
01_clus2	none		
.			
.			
.			

- b. Alternativamente, también puedes utilizar el `cluster ping-cluster -node <node-name>` Comando para comprobar la conectividad:

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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 3: Verificar la configuración

1. Verificar el estado de todos los puertos del clúster.

a. Puertos de clúster

- i. Compruebe que los puertos del clúster estén en buen estado en todos los nodos del clúster:

```
network port show ipspace Cluster
```

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

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

```
show cdp neighbors
```


Muestra el ejemplo

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

```
Node: node1-01
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: node1-02
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: node1-03
```

```
Ignore
```

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 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				
e7a	node1-01_clus1	up/up	169.254.209.69/16	node1-01
	true			
e7b	node1-01_clus2	up/up	169.254.49.125/16	node1-01
	true			
e7b	node1-02_clus1	up/up	169.254.47.194/16	node1-02
	true			
e7a	node1-02_clus2	up/up	169.254.19.183/16	node1-02
	true			
e7a	node1-03_clus1	up/up	169.254.209.69/16	node1-03
	true			
e7b	node1-03_clus2	up/up	169.254.49.125/16	node1-03
	true			
e7b	node1-04_clus1	up/up	169.254.47.194/16	node1-04
	true			
e7a	node1-04_clus2	up/up	169.254.19.183/16	node1-04
	false			

8 entries were displayed.

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

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

node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3
N9K-C9332D-GX2B			
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/4
N9K-C9332D-GX2B			
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/1
N9K-C9332D-GX2B			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/2
N9K-C9332D-GX2B			
	.		
	.		
	.		

```
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 Platform	Local Intrfce Port ID	Hldtme	Capability	
newcs2 (FDOXXXXXXXXX)	Eth1/31	179	R S I s	N9K-
C9364D-GX2A	Eth1/63			
newcs2 (FDOXXXXXXXXX)	Eth1/32	179	R S I s	N9K-
C9364D-GX2A	Eth1/64			

nodel-01	Eth1/4/1	123	H	AFX-1K
e1a				
nodel-01	Eth1/4/2	123	H	AFX-1K
e7a				
nodel-01	Eth1/4/3	123	H	AFX-1K
e10a				
nodel-01	Eth1/4/4	123	H	AFX-1K
e11a				
nodel-02	Eth1/9/1	138	H	AFX-1K
e1a				
nodel-02	Eth1/9/2	138	H	AFX-1K
e7a				
nodel-02	Eth1/9/3	138	H	AFX-1K
e10a				
nodel-02	Eth1/9/4	138	H	AFX-1K
e11a				
nodel-03	Eth1/15/1	138	H	AFX-1K
e1a				
nodel-03	Eth1/15/2	138	H	AFX-1K
e7a				
nodel-03	Eth1/15/3	138	H	AFX-1K
e10a				
nodel-03	Eth1/15/4	138	H	AFX-1K
e11a				
nodel-04	Eth1/16/1	173	H	AFX-1K
e1a				
nodel-04	Eth1/16/2	173	H	AFX-1K
e7a				
nodel-04	Eth1/16/3	173	H	AFX-1K
e10a				
nodel-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

newcs2# **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 (FDOXXXXXXXXX)  Eth1/31          179    R S I s    N9K-
C9364D-GX2A      Eth1/63
cs1 (FDOXXXXXXXXX)  Eth1/32          179    R S I s    N9K-
C9364D-GX2A      Eth1/64
node1-01          Eth1/4/1         123    H          AFX-1K
e1a
node1-01          Eth1/4/2         123    H          AFX-1K
e7a
node1-01          Eth1/4/3         123    H          AFX-1K
e10a
node1-01          Eth1/4/4         123    H          AFX-1K
e11a
node1-02          Eth1/9/1         138    H          AFX-1K
e1a
node1-02          Eth1/9/2         138    H          AFX-1K
e7a
node1-02          Eth1/9/3         138    H          AFX-1K
e10a
node1-02          Eth1/9/4         138    H          AFX-1K
e11a
node1-03          Eth1/15/1        138    H          AFX-1K
e1a
node1-03          Eth1/15/2        138    H          AFX-1K
e7a
node1-03          Eth1/15/3        138    H          AFX-1K
e10a
node1-03          Eth1/15/4        138    H          AFX-1K
e11a
node1-04          Eth1/16/1        173    H          AFX-1K
e1a
node1-04          Eth1/16/2        173    H          AFX-1K
e7a
node1-04          Eth1/16/3        173    H          AFX-1K
e10a
node1-04          Eth1/16/4        173    H          AFX-1K
e11a

```

Total entries displayed: 18

b. Puertos HA

i. Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf ID	Module	State	Internal?
1.1			
0	A	connected	false
1	A	connected	false
2	A	connected	false
3	A	connected	false
4	A	connected	false
5	A	connected	false
6	A	connected	false
7	A	connected	false
8	B	connected	false
9	B	connected	false
10	B	connected	false
11	B	connected	false
12	B	connected	false
13	B	connected	false
14	B	connected	false
15	B	connected	false

```
16 entries were displayed.
```

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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


Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

2. 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
```

El futuro

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

Cisco Nexus 9364D-GX2A

Manos a la obra

Flujo de trabajo de instalación y configuración para los conmutadores Cisco 9364D-GX2A

El conmutador Cisco 9364D-GX2A es parte de la plataforma Cisco Nexus 9000. Los conmutadores de sistemas AFX le permiten crear clústeres ONTAP con más de dos nodos.

Siga estos pasos de flujo de trabajo para instalar y configurar sus conmutadores Cisco 9364D-GX2A.

1

"Revisar los detalles del puerto del conmutador"

Revise los detalles del puerto del conmutador Cisco 9364D-GX2A.

2

"Revisar la documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores 9364D-GX2A y el clúster ONTAP .

3

"Revisar los requisitos de Smart Call Home"

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

4

"Instale el hardware"

Instale el hardware del interruptor.

5

"Configurar el software"

Configurar el software del conmutador.

Detalles del puerto para los conmutadores Cisco Nexus 9364D-GX2A

El conmutador Cisco Nexus 9364D-GX2A es parte de la plataforma Cisco Nexus 9000 y se puede instalar en un gabinete de sistema NetApp . Los conmutadores 9364D-GX2A le permiten crear clústeres ONTAP con más de dos nodos.

Detalles del puerto del Cisco Nexus 9364D-GX2A

Puertos	Descripción
Ethernet1/1/1-4 a Ethernet1/62/1-4	Modo 4x100GbE para conexiones de clúster, alta disponibilidad y almacenamiento AMD
Ethernet1/63, Ethernet1/64	400GbE ISL

Ver el ["Hardware Universe"](#) para obtener detalles de los puertos utilizados por la plataforma.

Requisitos de documentación para los conmutadores Cisco Nexus 9364D-GX2A

Para la instalación y el mantenimiento del conmutador Cisco Nexus 9364D-GX2A, asegúrese de revisar la documentación específica del conmutador y del controlador para configurar los conmutadores Cisco 9364D-GX2A y el clúster ONTAP .

Documentación de los switches

Para configurar los conmutadores Cisco Nexus 9364D-GX2A, necesita la siguiente documentación del ["Compatibilidad con los switches Cisco Nexus serie 9000"](#) página:

Título del documento	Descripción
"Guía de instalación del hardware del conmutador de modo NX-OS Cisco Nexus 9364D-GX2A"	Proporciona información detallada acerca de los requisitos del sitio, detalles del switch de hardware y las opciones de instalación.
"Guías de configuración del software del switch Cisco Nexus serie 9000" (seleccione la guía para la versión de NX-OS instalada en sus conmutadores)	Proporciona la información inicial de configuración del switch que necesita para poder configurar el switch para el funcionamiento de ONTAP.
"Guía de actualización y degradación del software Cisco Nexus serie 9000 NX-OS" (seleccione la guía para la versión de NX-OS instalada en sus conmutadores)	Proporciona información sobre cómo degradar el switch a software de switch compatible con ONTAP, si es necesario.
"Referencia de comandos NX-OS de Cisco Nexus serie 9000"	Proporciona vínculos a las diferentes referencias de comandos proporcionadas por Cisco.
"Referencia de mensajes del sistema NX-OS de Cisco Nexus serie 9000"	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.
"Notas de la versión de Cisco Nexus serie 9000 NX-OS" (seleccione las notas para la versión de NX-OS instalada en sus conmutadores)	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 de la ["Centro de documentación de ONTAP 9"](#) .

Nombre	Descripción
"Documentación de los sistemas AFX"	Describe cómo instalar el hardware de NetApp.

Nombre	Descripción
"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.

Requisitos de Smart Call Home

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

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

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

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

- Debe haber un servidor de correo electrónico.
- 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

Ir a la ["Flujo de trabajo de instalación y configuración de AFX"](#) para aprender cómo instalar y configurar el hardware del conmutador y el hardware del controlador para su sistema.

La documentación de instalación y configuración de AFX incluye información como:

- Instrucciones para preparar el sitio, desempacar las cajas y comparar el contenido de las cajas con el albarán, y registrar el sistema para acceder a los beneficios de soporte.
- Instrucciones para instalar los conmutadores, controladores y estantes de almacenamiento en un gabinete NetApp o un rack de telecomunicaciones.

- Instrucciones para cablear su sistema, incluido el cableado del almacenamiento del controlador para cambiar las conexiones y el cableado del estante para cambiar las conexiones.

Configurar el software

Configurar el flujo de trabajo del software para los conmutadores Cisco 9364D-GX2A

Para instalar y configurar el software de un conmutador Cisco 9364D-GX2A e instalar o actualizar el archivo de configuración de referencia (RCF), siga estos pasos:

1

"Configurar el conmutador 9364D-GX2A"

Configurar el conmutador Cisco 9364D-GX2A.

2

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

Instale el software Cisco NX-OS y los archivos de configuración de referencia (RCF) en los conmutadores Cisco 9364D-GX2A.

3

"Instale o actualice el software NX-OS"

Descargue e instale o actualice el software NX-OS en el conmutador Cisco 9364D-GX2A.

4

"Instale o actualice el RCF"

Instale o actualice el RCF después de configurar el conmutador Cisco 9364D-GX2A por primera vez. También puede utilizar este procedimiento para actualizar su versión de RCF.

5

"Verifique que SSH esté habilitado en los conmutadores Nexus 9364D-GX2A"

Verifique que SSH esté habilitado en el conmutador Cisco 9364D-GX2A para su uso con el Monitor de estado del conmutador Ethernet (CSHM) y las funciones de recopilación de registros.

6

"Restablecer el interruptor a los valores predeterminados de fábrica"

Borrar la configuración del conmutador Cisco 9364D-GX2A.

Una vez que haya terminado de configurar sus conmutadores, vaya a ["Encienda su sistema de almacenamiento AFX 1K"](#).

Configurar el conmutador 9364D-GX2A

Siga este procedimiento para configurar el conmutador Cisco Nexus 9364D-GX2A.

Antes de empezar

Asegúrese de tener:

- Encienda sus interruptores.

- 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.



- NX-OS 10.4.2 es la única versión compatible con los conmutadores Cisco Nexus 9364D-GX2A en un clúster ONTAP .
- No actualice ni degrade su versión de NX-OS a una versión no compatible; actualmente solo se admite la versión 10.4.2.

- Las licencias aplicables, la información de configuración y red, y los cables.
- Los RCF de red de gestión y red de clúster de NetApp aplicables descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#). 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.
- ["Documentación necesaria sobre el switch y ONTAP"](#) .

Pasos

1. 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

Prompt	Respuesta
¿Configurar cadena de comunidad SNMP de lectura y escritura? (sí/no)	Responda con no . El valor predeterminado es no
Introduzca el nombre del switch.	Introduzca el nombre del switch, que 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
¿Habilitar el servicio telnet? (sí/no)	Responda con no . El valor predeterminado es no
¿Servicio SSH habilitado? (sí/no)	Responda con sí. El valor predeterminado es yes.  Se recomienda SSH cuando se utiliza Ethernet Switch Health Monitor (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.
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 a 2048.
¿Configurar el servidor NTP? (sí/no)	Responda con no . El valor predeterminado es no
Configuración de 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.

Prompt	Respuesta
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)	Responda con sí para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.  Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador.

- 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

Después de haber configurado sus conmutadores, ["Prepárese para instalar NX-OS y RCF"](#) .

Prepárese para instalar el software NX-OS y RCF

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

Acerca de los ejemplos

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

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de los nodos son node1-01, node1-02, node1-03 y node1-04.
- Los nombres del clúster LIF son:
 - node1-01_clus1 y node1-01_clus2 para node1-01
 - node1-02_clus1 y node1-02_clus2 para node1-02
 - node1-03_clus1 y node1-03_clus2 para node1-03
 - node1-04_clus1 y node1-04_clus2 para node1-04
- 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.

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. Consulta el estado administrativo y operativo de cada puerto.

a. Puertos de clúster

- i. 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

node1-02/cdp			
	e10a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/3
N9K-C9364D-GX2A			
	e10b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/3
N9K-C9364D-GX2A			
	e11a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/4
N9K-C9364D-GX2A			
	e11b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/4
N9K-C9364D-GX2A			
	e1a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/1
N9K-C9364D-GX2A			
	e1b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/1
N9K-C9364D-GX2A			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/2
N9K-C9364D-GX2A			
	e7b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/2
N9K-C9364D-GX2A			
node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/3
N9K-C9364D-GX2A			
	e10b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/3
N9K-C9364D-GX2A			
	e11a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/4
N9K-C9364D-GX2A			
	e11b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/4
N9K-C9364D-GX2A			
	e1a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/1
N9K-C9364D-GX2A			
	e1b	cs2 (FDOXXXXXXXXXX)	Ethernet1/13/1
N9K-C9364D-GX2A			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXXX)	Ethernet1/16/2

```
N9K-C9364D-GX2A
```

```
e7b
```

```
cs2 (FDOXXXXXXXX)
```

```
Ethernet1/13/2
```

```
N9K-C9364D-GX2A
```

```
.
```

```
.
```

```
.
```

ii. Mostrar los atributos del puerto de red:

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

Muestra el ejemplo

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

Node: node1-01

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000

```
healthy false
```

```
Node: nodel-04
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy false						
e7b	Cluster	Cluster		up	9000	auto/100000
healthy false						

```
8 entries were displayed.
```

iii. Mostrar información sobre los LIF del clúster:

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

```
8 entries were displayed.
```

b. Puertos HA

i. Mostrar información sobre los puertos HA:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

- i. Mostrar información sobre los puertos de almacenamiento:

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

Muestra el ejemplo

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

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

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

4. Verificar la conectividad de las interfaces del clúster remoto.

- Puedes utilizar el `network interface check cluster-connectivity show` Comando para mostrar los detalles de una verificación de accesibilidad para la conectividad del clúster:

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

Muestra el ejemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-02_clus1
none			
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-02_clus1
none			
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-01_clus1
none			
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-01_clus2
none			
.			
.			
.			

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

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node1-04
Getting addresses from network interface table...
Cluster node1-01_clus1 169.254.36.44 node1-01 e7a
Cluster node1-01_clus2 169.254.7.5 node1-01 e7b
Cluster node1-02_clus1 169.254.197.206 node1-02 e7a
Cluster node1-02_clus2 169.254.195.186 node1-02 e7b
Cluster node1-03_clus1 169.254.192.49 node1-03 e7a
Cluster node1-03_clus2 169.254.182.76 node1-03 e7b
Cluster node1-04_clus1 169.254.59.49 node1-04 e7a
Cluster node1-04_clus2 169.254.62.244 node1-04 e7b
Local = 169.254.59.49 169.254.62.244
Remote = 169.254.36.44 169.254.7.5 169.254.197.206 169.254.195.186
169.254.192.49 169.254.182.76
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 169.254.59.49 to Remote 169.254.182.76
    Local 169.254.59.49 to Remote 169.254.192.49
    Local 169.254.59.49 to Remote 169.254.195.186
    Local 169.254.59.49 to Remote 169.254.197.206
    Local 169.254.59.49 to Remote 169.254.36.44
    Local 169.254.59.49 to Remote 169.254.7.5
    Local 169.254.62.244 to Remote 169.254.182.76
    Local 169.254.62.244 to Remote 169.254.192.49
    Local 169.254.62.244 to Remote 169.254.195.186
    Local 169.254.62.244 to Remote 169.254.197.206
    Local 169.254.62.244 to Remote 169.254.36.44
    Local 169.254.62.244 to Remote 169.254.7.5
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)
```

5. Verifique que el comando de reversión automática esté habilitado en todos los 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	node1-01_clus1	true
Cluster	node1-01_clus2	true
Cluster	node1-02_clus1	true
Cluster	node1-02_clus2	true
Cluster	node1-03_clus1	true
Cluster	node1-03_clus2	true
Cluster	node1-04_clus1	true
Cluster	node1-04_clus2	true

8 entries were displayed.

El futuro

Una vez que se haya preparado para instalar el software NX-OS y RCF, debe ["instalar o actualizar el software NX-OS"](#) .

Instale o actualice el software NX-OS

Siga este procedimiento para instalar o actualizar el software NX-OS en el conmutador Nexus 9364D-GX2A.

Revise los requisitos

Antes de empezar

Verifique lo siguiente:

- Complete el procedimiento en ["Prepare la instalación de NX-OS y RCF"](#) .
- Está disponible una copia de seguridad actual de la configuración del conmutador.
- Se ha instalado un clúster en pleno funcionamiento (sin errores en los registros ni problemas similares).

Documentación sugerida

- ["Página del switch Cisco Ethernet"](#)

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

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

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

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

Proporciona información sobre actualización/degradación disruptiva para software Cisco NX-OS en los switches de la serie Nexus 9000 en función de tus versiones actuales y objetivo.

En la página, selecciona **Actualización disruptiva** y selecciona tu versión actual y la versión de destino de la lista desplegable.

Acerca de los ejemplos

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

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

Instale el software

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.



- NX-OS 10.4.2 es la única versión compatible con los conmutadores Cisco Nexus 9364D-GX2A en un clúster ONTAP .
- No actualice ni degrade su versión de NX-OS a una versión no compatible; actualmente solo se admite la versión 10.4.2.

Pasos

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

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

node1-01/cdp				
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9364D-GX2A				
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/3	N9K-
C9364D-GX2A				
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-
C9364D-GX2A				
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/4	N9K-
C9364D-GX2A				
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1	N9K-
C9364D-GX2A				
	e1b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/1	N9K-
C9364D-GX2A				
	.			
	.			
	.			
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2	N9K-
C9364D-GX2A				
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/2	N9K-
C9364D-GX2A				
node1-01/lldp				
	e10a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/3	-
	e10b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/13/3	-
	e11a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/4	-
	e11b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/13/4	-
	e1a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/1	-
	e1b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/13/1	-
	.			
	.			
	.			
	e7a	cs1 (c8:60:8f:xx:xx:xx)	Ethernet1/16/2	-
	e7b	cs2 (04:e3:87:xx:xx:xx)	Ethernet1/13/2	-
	.			
	.			
	.			

4. Consulta el estado administrativo y operativo de cada puerto.

a. **Puertos de clúster**

i. 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: node1-01

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-02

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

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

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

8 entries were displayed.

iii. 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

cs2 (FDOXXXXXXXXX) N9K-C9364D-GX2A	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
cs1 (FLMXXXXXXXXX) N9K-C9364D-GX2A	cluster-network	10.228.137.253
Serial Number: FLMXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
10.4(2)		
Version Source: CDP/ISDP		
2 entries were displayed.		

b. Puertos HA

- Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01  
(system ha interconnect status show)
```

```
Node: node1-01  
Link 0 Status: up  
Link 1 Status: up  
Is Link 0 Active: true  
Is Link 1 Active: true  
IC RDMA Connection: up  
Slot: 0  
Debug Firmware: no
```

```
Interconnect Port 0 :  
Port Name: ela-17  
MTU: 4096  
Link Information: ACTIVE
```

```
Interconnect Port 1 :  
Port Name: elb-18  
MTU: 4096  
Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02  
(system ha interconnect status show)
```

```
Node: node1-02  
Link 0 Status: up  
Link 1 Status: up  
Is Link 0 Active: true  
Is Link 1 Active: true  
IC RDMA Connection: up  
Slot: 0  
Debug Firmware: no
```

```
Interconnect Port 0 :  
Port Name: ela-17  
MTU: 4096  
Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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


Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

```
16 entries were displayed.
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

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

6. Copie el software NX-OS y las imágenes EPLD al conmutador Nexus 9364D-GX2A.

Muestra el ejemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.10.4.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: root

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
root@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.10.4.2.bin /bootflash/nxos.10.4.2.bin
/code/nxos.10.4.2.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.10.4.2.F.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.10.4.2.F.img /bootflash/n9000-
epld.10.4.2.F.img
/code/n9000-epld.10.4.2.F.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

```
show version
```

```
cs2# show version
```

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2025, 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 01.14
NXOS: version 10.4(1) [Feature Release]
Host NXOS: version 10.4(1)
BIOS compile time: 11/25/2024
NXOS image file is: bootflash:///nxos64-cs.10.4.1.F.bin
NXOS compile time: 11/30/2023 12:00:00 [12/14/2023 05:25:50]
NXOS boot mode: LXC
```

Hardware

```
cisco Nexus9000 C9332D-GX2B Chassis
Intel(R) Xeon(R) CPU D-1633N @ 2.50GHz with 32802156 kB of memory.
Processor Board ID FLMXXXXXXXXX
Device name: cs2
bootflash: 115802886 kB
```

```
Kernel uptime is 5 day(s), 2 hour(s), 13 minute(s), 21 second(s)
```

```
Last reset at 3580 usecs after Thu Jun  5 15:55:08 2025
```

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

```
System version: 10.4(1)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

8. 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.10.4.2.bin
```

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

```
Verifying image bootflash:/nxos.10.4.2.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

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

```
Preparing "nxos" version info using image  
bootflash:/nxos.10.4.2.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image  
bootflash:/nxos.10.4.2.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	10.4 (1)	10.4 (2)
Yes			
1	bios	xx.xx.:xx.xx	xxx
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.

9. 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) 2002-2025, 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 01.14
NXOS: version 10.4(2) [Feature Release]
Host NXOS: version 10.4(2)
BIOS compile time: 11/25/2024
NXOS image file is: bootflash:///nxos64-cs.10.4.2.F.bin
NXOS compile time: 11/30/2023 12:00:00 [12/14/2023 05:25:50]
NXOS boot mode: LXC
```

Hardware

```
cisco Nexus9000 C9332D-GX2B Chassis
Intel(R) Xeon(R) CPU D-1633N @ 2.50GHz with 32802156 kB of memory.
Processor Board ID FLMXXXXXXXXX
Device name: cs2
bootflash: 115802886 kB
```

```
Kernel uptime is 5 day(s), 2 hour(s), 13 minute(s), 21 second(s)
```

```
Last reset at 3580 usecs after Thu Jun 5 15:55:08 2025
```

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

```
System version: 10.4(2)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

10. 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.10.4.2.F.img module all
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

11. Tras reiniciar el 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

12. Verificar el estado de todos los puertos del clúster.

a. Puertos de clúster

- i. 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: node1-01

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

ii. Compruebe el estado del switch del clúster:

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

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

Muestra el ejemplo

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

node1-01/cdp
      e10a  cs1 (FLMXXXXXXXXXX)      Ethernet1/16/3
N9K-C9364D-GX2A
      e10b  cs2 (FDOXXXXXXXXXX)      Ethernet1/13/3
N9K-C9364D-GX2A
      e11a  cs1 (FLMXXXXXXXXXX)      Ethernet1/16/4
N9K-C9364D-GX2A
      e11b  cs2 (FDOXXXXXXXXXX)      Ethernet1/13/4
N9K-C9364D-GX2A
      e1a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/1
N9K-C9364D-GX2A
      e1b   cs2 (FDOXXXXXXXXXX)      Ethernet1/13/1
N9K-C9364D-GX2A
      .
      .
      .
      e7a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/2
N9K-C9364D-GX2A
      e7b   cs2 (FDOXXXXXXXXXX)      Ethernet1/13/2
N9K-C9364D-GX2A

node1-02/cdp
      e10a  cs1 (FLMXXXXXXXXXX)      Ethernet1/16/3
N9K-C9364D-GX2A
      e10b  cs2 (FDOXXXXXXXXXX)      Ethernet1/13/3
N9K-C9364D-GX2A
      e11a  cs1 (FLMXXXXXXXXXX)      Ethernet1/16/4
N9K-C9364D-GX2A
      e11b  cs2 (FDOXXXXXXXXXX)      Ethernet1/13/4
N9K-C9364D-GX2A
      e1a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/1
N9K-C9364D-GX2A
      e1b   cs2 (FDOXXXXXXXXXX)      Ethernet1/13/1
N9K-C9364D-GX2A
      .
      .
      .
      e7a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/2
N9K-C9364D-GX2A
      e7b   cs2 (FDOXXXXXXXXXX)      Ethernet1/13/2
N9K-C9364D-GX2A
      .
```

```

.
.

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                Type                                Address
Model
-----
cs2 (FDOXXXXXXXXX)                   cluster-network                   10.228.137.233
N9K-C9364D-GX2A
    Serial Number: FDOXXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

cs1 (FLMXXXXXXXXX)                   cluster-network                   10.228.137.253
N9K-C9364D-GX2A
    Serial Number: FLMXXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

```

b. Puertos HA

- i. Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```



```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

.
.
.

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online

16 entries were displayed.

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

13. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	false
node1-04	true	true	true

4 entries were displayed.

14. Repita los pasos 6 a 13 para instalar el software NX-OS en el interruptor CS1.

15. Habilite la reversión automática en las LIF del clúster.

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

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

Si alguna LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

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

El futuro

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

Instale o actualice el RCF

Instale o actualice la descripción general del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar el conmutador Nexus 9364D-GX2A por primera vez. Actualiza tu versión RCF cuando tienes una versión existente del archivo RCF instalado en tu conmutador.

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

Configuración RCF disponible

- **Cluster-HA-Storage:** admite tráfico compartido de clúster/HA/almacenamiento en puertos (NX9364D-GX2A-RCF-v10.0-Shared.txt).

Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

Documentación sugerida

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

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

- [Conmutadores Cisco Nexus 3=9000 Series](#)

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

Acerca de los ejemplos

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

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

Ver el ["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.

Comandos utilizados

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.

El futuro

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

Instalación del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar el conmutador Nexus 9364D-GX2A por primera vez.

Antes de empezar

Compruebe las siguientes instalaciones y conexiones:

- Una conexión de consola al interruptor. La conexión de la consola es opcional si tiene acceso remoto al conmutador.
- El switch CS1 y el switch CS2 se encienden y la configuración inicial del switch se ha completado (la dirección IP de gestión y SSH está configurado).
- Se ha instalado la versión deseada de NX-OS.
- Las conexiones ISL entre los switches están conectadas.
- Los puertos del clúster de nodos de ONTAP no están conectados.

Paso 1: Instale el RCF en los interruptores

1. Inicie sesión en el switch CS1 mediante SSH o mediante una consola de serie.
2. Copie el RCF al bootflash del switch CS1 usando 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 9000"](#) guías.

Muestra el ejemplo

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: NX9364D-GX2A-RCF-v10.0-Shared.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

3. Aplique el RCF descargado 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 9000"](#) guías.

Muestra el ejemplo

Este ejemplo muestra el archivo RCF NX9364D-GX2A-RCF-v10.0-Shared.txt siendo instalado en el switch cs1:

```
cs1# copy NX9364D-GX2A-RCF-v10.0-Shared.txt running-config echo-  
commands
```

4. Examine el resultado del banner desde el `show banner motd` comando. Debe leer y seguir estas instrucciones para asegurarse de que la configuración y el funcionamiento del interruptor son correctos.

Muestra el ejemplo

```
cs1# show banner motd  
  
*****  
*****  
* NetApp Reference Configuration File (RCF)  
*  
* Switch    : NX9364D-GX2A  
* Filename  : NX9364D-GX2A-RCF-v10.0-Shared.txt  
* Date      : 05-09-2025  
* Version   : v10.0  
* Port Usage:  
* Ports 1-62: 100GbE Intra-Cluster/HA/Storage Ports, int e1/{1-  
62}/1-4  
* Ports 63-64: Intra-Cluster ISL Ports, int e1/63-64  
*  
* IMPORTANT NOTES  
* Interface port-channel999 is reserved to identify the version of  
this file.  
*  
*****  
*****
```

5. 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.

6. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.



Asegúrese de configurar lo siguiente:

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

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

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

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

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

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

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

cs1# echo "hardware access-list tcam region ing-l2-qos 1536" >>
bootflash:write_erase.cfg
```

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

7. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

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

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

```
cs1# write erase
```

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

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

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

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

10. Reinicie el switch:


```
cs1# reload
```

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

11. Repita los pasos 1 al 10 en el interruptor cs2.
12. Conecte los puertos de todos los nodos del clúster ONTAP a los conmutadores cs1 y cs2.

Paso 2: Verifique las conexiones del interruptor

1. Verifique que los puertos del conmutador conectados a los puertos del clúster estén activos:

```
show interface brief
```

Muestra el ejemplo

```
cs1# show interface brief | grep up
.
.
Eth1/9/3          1          eth  trunk  up      none
100G(D) --
Eth1/9/4          1          eth  trunk  up      none
100G(D) --
Eth1/15/1         1          eth  trunk  up      none
100G(D) --
Eth1/15/2         1          eth  trunk  up      none
100G(D) --
Eth1/15/3         1          eth  trunk  up      none
100G(D) --
Eth1/15/4         1          eth  trunk  up      none
100G(D) --
Eth1/16/1         1          eth  trunk  up      none
100G(D) --
Eth1/16/2         1          eth  trunk  up      none
100G(D) --
Eth1/16/3         1          eth  trunk  up      none
100G(D) --
Eth1/16/4         1          eth  trunk  up      none
100G(D) --
Eth1/17/1         1          eth  trunk  up      none
100G(D) --
Eth1/17/2         1          eth  trunk  up      none
100G(D) --
Eth1/17/3         1          eth  trunk  up      none
100G(D) --
Eth1/17/4         1          eth  trunk  up      none
100G(D) --
.
.
```

2. Compruebe que los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Po999, Eth1/63, Eth1/64 Eth1/65, Eth1/66, Eth1/1/1 Eth1/1/2, Eth1/1/3, Eth1/1/4 Eth1/2/1, Eth1/2/2, Eth1/2/3 Eth1/2/4, Eth1/3/1, Eth1/3/2 Eth1/3/3, Eth1/3/4, Eth1/4/1 Eth1/4/2, Eth1/4/3, Eth1/4/4 Eth1/5/1, Eth1/5/2, Eth1/5/3 Eth1/5/4, Eth1/6/1, Eth1/6/2 Eth1/6/3, Eth1/6/4, Eth1/7/1 Eth1/7/2, Eth1/7/3, Eth1/7/4 Eth1/8/1, Eth1/8/2, Eth1/8/3 Eth1/8/4, Eth1/9/1, Eth1/9/2 Eth1/9/3, Eth1/9/4, Eth1/10/1 Eth1/10/2, Eth1/10/3, Eth1/10/4 Eth1/11/1, Eth1/11/2, Eth1/11/3 Eth1/11/4, Eth1/12/1, Eth1/12/2 Eth1/12/3, Eth1/12/4, Eth1/13/1 Eth1/13/2, Eth1/13/3, Eth1/13/4 Eth1/14/1,

Eth1/14/2, Eth1/14/3

Eth1/15/1, Eth1/15/2

Eth1/15/4, Eth1/16/1

Eth1/16/3, Eth1/16/4

Eth1/17/2, Eth1/17/3

Eth1/18/1, Eth1/18/2

Eth1/18/4, Eth1/19/1

Eth1/19/3, Eth1/19/4

Eth1/20/2, Eth1/20/3

Eth1/21/1, Eth1/21/2

Eth1/21/4, Eth1/22/1

Eth1/22/3, Eth1/22/4

Eth1/23/2, Eth1/23/3

Eth1/24/1, Eth1/24/2

Eth1/24/4, Eth1/25/1

Eth1/25/3, Eth1/25/4

Eth1/26/2, Eth1/26/3

Eth1/27/1, Eth1/27/2

Eth1/27/4, Eth1/28/1

Eth1/28/3, Eth1/28/4

Eth1/29/2, Eth1/29/3

Eth1/30/1, Eth1/30/2

Eth1/30/4, Eth1/31/1

Eth1/14/4,

Eth1/15/3,

Eth1/16/2,

Eth1/17/1,

Eth1/17/4,

Eth1/18/3,

Eth1/19/2,

Eth1/20/1,

Eth1/20/4,

Eth1/21/3,

Eth1/22/2,

Eth1/23/1,

Eth1/23/4,

Eth1/24/3,

Eth1/25/2,

Eth1/26/1,

Eth1/26/4,

Eth1/27/3,

Eth1/28/2,

Eth1/29/1,

Eth1/29/4,

Eth1/30/3,

Eth1/31/2,

Eth1/31/3, Eth1/31/4

Eth1/32/2, Eth1/32/3

Eth1/33/1, Eth1/33/2

Eth1/33/4, Eth1/34/1

Eth1/34/3, Eth1/34/4

Eth1/35/2, Eth1/35/3

Eth1/36/1, Eth1/36/2

Eth1/36/4, Eth1/37/1

Eth1/37/3, Eth1/37/4

Eth1/38/2, Eth1/38/3

Eth1/39/1, Eth1/39/2

Eth1/39/4, Eth1/40/1

Eth1/40/3, Eth1/40/4

Eth1/41/2, Eth1/41/3

Eth1/42/1, Eth1/42/2

Eth1/42/4, Eth1/43/1

Eth1/43/3, Eth1/43/4

Eth1/44/2, Eth1/44/3

Eth1/45/1, Eth1/45/2

Eth1/45/4, Eth1/46/1

Eth1/46/3, Eth1/46/4

Eth1/47/2, Eth1/47/3

Eth1/48/1, Eth1/48/2

Eth1/32/1,

Eth1/32/4,

Eth1/33/3,

Eth1/34/2,

Eth1/35/1,

Eth1/35/4,

Eth1/36/3,

Eth1/37/2,

Eth1/38/1,

Eth1/38/4,

Eth1/39/3,

Eth1/40/2,

Eth1/41/1,

Eth1/41/4,

Eth1/42/3,

Eth1/43/2,

Eth1/44/1,

Eth1/44/4,

Eth1/45/3,

Eth1/46/2,

Eth1/47/1,

Eth1/47/4,

Eth1/48/3,

Eth1/48/4, Eth1/49/1		Eth1/49/2,
Eth1/49/3, Eth1/49/4		Eth1/50/1,
Eth1/50/2, Eth1/50/3		Eth1/50/4,
Eth1/51/1, Eth1/51/2		Eth1/51/3,
Eth1/51/4, Eth1/52/1		Eth1/52/2,
Eth1/52/3, Eth1/52/4		Eth1/53/1,
Eth1/53/2, Eth1/53/3		Eth1/53/4,
Eth1/54/1, Eth1/54/2		Eth1/54/3,
Eth1/54/4, Eth1/55/1		Eth1/55/2,
Eth1/55/3, Eth1/55/4		Eth1/56/1,
Eth1/56/2, Eth1/56/3		Eth1/56/4,
Eth1/57/1, Eth1/57/2		Eth1/57/3,
Eth1/57/4, Eth1/58/1		Eth1/58/2,
Eth1/58/3, Eth1/58/4		Eth1/59/1,
Eth1/59/2, Eth1/59/3		Eth1/59/4,
Eth1/60/1, Eth1/60/2		Eth1/60/3,
Eth1/60/4, Eth1/61/1		Eth1/61/2,
Eth1/61/3, Eth1/61/4		Eth1/62/1,
Eth1/62/2, Eth1/62/3		Eth1/62/4
17 VLAN0017	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		

Eth1/4/3	Eth1/4/1, Eth1/4/2,
Eth1/5/2	Eth1/4/4, Eth1/5/1,
Eth1/6/1	Eth1/5/3, Eth1/5/4,
Eth1/6/4	Eth1/6/2, Eth1/6/3,
Eth1/7/3	Eth1/7/1, Eth1/7/2,
Eth1/8/2	Eth1/7/4, Eth1/8/1,
Eth1/9/1	Eth1/8/3, Eth1/8/4,
Eth1/9/4	Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3	Eth1/10/1,
Eth1/11/1, Eth1/11/2	Eth1/10/4,
Eth1/11/4, Eth1/12/1	Eth1/11/3,
Eth1/12/3, Eth1/12/4	Eth1/12/2,
Eth1/13/2, Eth1/13/3	Eth1/13/1,
Eth1/14/1, Eth1/14/2	Eth1/13/4,
Eth1/14/4, Eth1/15/1	Eth1/14/3,
Eth1/15/3, Eth1/15/4	Eth1/15/2,
Eth1/16/2, Eth1/16/3	Eth1/16/1,
Eth1/17/1, Eth1/17/2	Eth1/16/4,
Eth1/17/4, Eth1/18/1	Eth1/17/3,
Eth1/18/3, Eth1/18/4	Eth1/18/2,
Eth1/19/2, Eth1/19/3	Eth1/19/1,
Eth1/20/1, Eth1/20/2	Eth1/19/4,
Eth1/20/4, Eth1/21/1	Eth1/20/3,

Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4
Eth1/31/2, Eth1/31/3
Eth1/32/1, Eth1/32/2
Eth1/32/4, Eth1/33/1
Eth1/33/3, Eth1/33/4
Eth1/34/2, Eth1/34/3
Eth1/35/1, Eth1/35/2
Eth1/35/4, Eth1/36/1
Eth1/36/3, Eth1/36/4
Eth1/37/2, Eth1/37/3
Eth1/38/1, Eth1/38/2

Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,
Eth1/31/1,
Eth1/31/4,
Eth1/32/3,
Eth1/33/2,
Eth1/34/1,
Eth1/34/4,
Eth1/35/3,
Eth1/36/2,
Eth1/37/1,
Eth1/37/4,

Eth1/38/4, Eth1/39/1
Eth1/39/3, Eth1/39/4
Eth1/40/2, Eth1/40/3
Eth1/41/1, Eth1/41/2
Eth1/41/4, Eth1/42/1
Eth1/42/3, Eth1/42/4
Eth1/43/2, Eth1/43/3
Eth1/44/1, Eth1/44/2
Eth1/44/4, Eth1/45/1
Eth1/45/3, Eth1/45/4
Eth1/46/2, Eth1/46/3
Eth1/47/1, Eth1/47/2
Eth1/47/4, Eth1/48/1
Eth1/48/3, Eth1/48/4
Eth1/49/2, Eth1/49/3
Eth1/50/1, Eth1/50/2
Eth1/50/4, Eth1/51/1
Eth1/51/3, Eth1/51/4
Eth1/52/2, Eth1/52/3
Eth1/53/1, Eth1/53/2
Eth1/53/4, Eth1/54/1
Eth1/54/3, Eth1/54/4
Eth1/55/2, Eth1/55/3

Eth1/38/3,
Eth1/39/2,
Eth1/40/1,
Eth1/40/4,
Eth1/41/3,
Eth1/42/2,
Eth1/43/1,
Eth1/43/4,
Eth1/44/3,
Eth1/45/2,
Eth1/46/1,
Eth1/46/4,
Eth1/47/3,
Eth1/48/2,
Eth1/49/1,
Eth1/49/4,
Eth1/50/3,
Eth1/51/2,
Eth1/52/1,
Eth1/52/4,
Eth1/53/3,
Eth1/54/2,
Eth1/55/1,

Eth1/56/1, Eth1/56/2		Eth1/55/4,
Eth1/56/4, Eth1/57/1		Eth1/56/3,
Eth1/57/3, Eth1/57/4		Eth1/57/2,
Eth1/58/2, Eth1/58/3		Eth1/58/1,
Eth1/59/1, Eth1/59/2		Eth1/58/4,
Eth1/59/4, Eth1/60/1		Eth1/59/3,
Eth1/60/3, Eth1/60/4		Eth1/60/2,
Eth1/61/2, Eth1/61/3		Eth1/61/1,
Eth1/62/1, Eth1/62/2		Eth1/61/4,
18 VLAN0018	active	Eth1/62/3, Eth1/62/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
Eth1/2/2		Eth1/1/4, Eth1/2/1,
Eth1/3/1		Eth1/2/3, Eth1/2/4,
Eth1/3/4		Eth1/3/2, Eth1/3/3,
Eth1/4/3		Eth1/4/1, Eth1/4/2,
Eth1/5/2		Eth1/4/4, Eth1/5/1,
Eth1/6/1		Eth1/5/3, Eth1/5/4,
Eth1/6/4		Eth1/6/2, Eth1/6/3,
Eth1/7/3		Eth1/7/1, Eth1/7/2,
Eth1/8/2		Eth1/7/4, Eth1/8/1,
Eth1/9/1		Eth1/8/3, Eth1/8/4,
Eth1/9/4		Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3		Eth1/10/1,
		Eth1/10/4,

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/31/2, Eth1/31/3

Eth1/32/1, Eth1/32/2

Eth1/32/4, Eth1/33/1

Eth1/33/3, Eth1/33/4

Eth1/34/2, Eth1/34/3

Eth1/35/1, Eth1/35/2

Eth1/35/4, Eth1/36/1

Eth1/36/3, Eth1/36/4

Eth1/37/2, Eth1/37/3

Eth1/38/1, Eth1/38/2

Eth1/38/4, Eth1/39/1

Eth1/39/3, Eth1/39/4

Eth1/40/2, Eth1/40/3

Eth1/41/1, Eth1/41/2

Eth1/41/4, Eth1/42/1

Eth1/42/3, Eth1/42/4

Eth1/43/2, Eth1/43/3

Eth1/44/1, Eth1/44/2

Eth1/44/4, Eth1/45/1

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

Eth1/31/1,

Eth1/31/4,

Eth1/32/3,

Eth1/33/2,

Eth1/34/1,

Eth1/34/4,

Eth1/35/3,

Eth1/36/2,

Eth1/37/1,

Eth1/37/4,

Eth1/38/3,

Eth1/39/2,

Eth1/40/1,

Eth1/40/4,

Eth1/41/3,

Eth1/42/2,

Eth1/43/1,

Eth1/43/4,

Eth1/44/3,

Eth1/45/2,

Eth1/45/3, Eth1/45/4

Eth1/46/2, Eth1/46/3

Eth1/47/1, Eth1/47/2

Eth1/47/4, Eth1/48/1

Eth1/48/3, Eth1/48/4

Eth1/49/2, Eth1/49/3

Eth1/50/1, Eth1/50/2

Eth1/50/4, Eth1/51/1

Eth1/51/3, Eth1/51/4

Eth1/52/2, Eth1/52/3

Eth1/53/1, Eth1/53/2

Eth1/53/4, Eth1/54/1

Eth1/54/3, Eth1/54/4

Eth1/55/2, Eth1/55/3

Eth1/56/1, Eth1/56/2

Eth1/56/4, Eth1/57/1

Eth1/57/3, Eth1/57/4

Eth1/58/2, Eth1/58/3

Eth1/59/1, Eth1/59/2

Eth1/59/4, Eth1/60/1

Eth1/60/3, Eth1/60/4

Eth1/61/2, Eth1/61/3

Eth1/62/1, Eth1/62/2

Eth1/46/1,

Eth1/46/4,

Eth1/47/3,

Eth1/48/2,

Eth1/49/1,

Eth1/49/4,

Eth1/50/3,

Eth1/51/2,

Eth1/52/1,

Eth1/52/4,

Eth1/53/3,

Eth1/54/2,

Eth1/55/1,

Eth1/55/4,

Eth1/56/3,

Eth1/57/2,

Eth1/58/1,

Eth1/58/4,

Eth1/59/3,

Eth1/60/2,

Eth1/61/1,

Eth1/61/4,

Eth1/62/3, Eth1/62/4

30	VLAN0030	active	Eth1/1/1, Eth1/1/2,
	Eth1/1/3		Eth1/1/4, Eth1/2/1,
	Eth1/2/2		Eth1/2/3, Eth1/2/4,
	Eth1/3/1		Eth1/3/2, Eth1/3/3,
	Eth1/3/4		Eth1/4/1, Eth1/4/2,
	Eth1/4/3		Eth1/4/4, Eth1/5/1,
	Eth1/5/2		Eth1/5/3, Eth1/5/4,
	Eth1/6/1		Eth1/6/2, Eth1/6/3,
	Eth1/6/4		Eth1/7/1, Eth1/7/2,
	Eth1/7/3		Eth1/7/4, Eth1/8/1,
	Eth1/8/2		Eth1/8/3, Eth1/8/4,
	Eth1/9/1		Eth1/9/2, Eth1/9/3,
	Eth1/9/4		Eth1/10/1,
	Eth1/10/2, Eth1/10/3		Eth1/10/4,
	Eth1/11/1, Eth1/11/2		Eth1/11/3,
	Eth1/11/4, Eth1/12/1		Eth1/12/2,
	Eth1/12/3, Eth1/12/4		Eth1/13/1,
	Eth1/13/2, Eth1/13/3		Eth1/13/4,
	Eth1/14/1, Eth1/14/2		Eth1/14/3,
	Eth1/14/4, Eth1/15/1		Eth1/15/2,
	Eth1/15/3, Eth1/15/4		Eth1/16/1,
	Eth1/16/2, Eth1/16/3		Eth1/16/4,
	Eth1/17/1, Eth1/17/2		Eth1/17/3,
	Eth1/17/4, Eth1/18/1		

Eth1/18/3, Eth1/18/4
Eth1/19/2, Eth1/19/3
Eth1/20/1, Eth1/20/2
Eth1/20/4, Eth1/21/1
Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4
Eth1/31/2, Eth1/31/3
Eth1/32/1, Eth1/32/2
Eth1/32/4, Eth1/33/1
Eth1/33/3, Eth1/33/4
Eth1/34/2, Eth1/34/3
Eth1/35/1, Eth1/35/2

Eth1/18/2,
Eth1/19/1,
Eth1/19/4,
Eth1/20/3,
Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,
Eth1/31/1,
Eth1/31/4,
Eth1/32/3,
Eth1/33/2,
Eth1/34/1,
Eth1/34/4,

Eth1/35/4, Eth1/36/1
Eth1/36/3, Eth1/36/4
Eth1/37/2, Eth1/37/3
Eth1/38/1, Eth1/38/2
Eth1/38/4, Eth1/39/1
Eth1/39/3, Eth1/39/4
Eth1/40/2, Eth1/40/3
Eth1/41/1, Eth1/41/2
Eth1/41/4, Eth1/42/1
Eth1/42/3, Eth1/42/4
Eth1/43/2, Eth1/43/3
Eth1/44/1, Eth1/44/2
Eth1/44/4, Eth1/45/1
Eth1/45/3, Eth1/45/4
Eth1/46/2, Eth1/46/3
Eth1/47/1, Eth1/47/2
Eth1/47/4, Eth1/48/1
Eth1/48/3, Eth1/48/4
Eth1/49/2, Eth1/49/3
Eth1/50/1, Eth1/50/2
Eth1/50/4, Eth1/51/1
Eth1/51/3, Eth1/51/4
Eth1/52/2, Eth1/52/3

Eth1/35/3,
Eth1/36/2,
Eth1/37/1,
Eth1/37/4,
Eth1/38/3,
Eth1/39/2,
Eth1/40/1,
Eth1/40/4,
Eth1/41/3,
Eth1/42/2,
Eth1/43/1,
Eth1/43/4,
Eth1/44/3,
Eth1/45/2,
Eth1/46/1,
Eth1/46/4,
Eth1/47/3,
Eth1/48/2,
Eth1/49/1,
Eth1/49/4,
Eth1/50/3,
Eth1/51/2,
Eth1/52/1,

Eth1/53/1, Eth1/53/2		Eth1/52/4,
Eth1/53/4, Eth1/54/1		Eth1/53/3,
Eth1/54/3, Eth1/54/4		Eth1/54/2,
Eth1/55/2, Eth1/55/3		Eth1/55/1,
Eth1/56/1, Eth1/56/2		Eth1/55/4,
Eth1/56/4, Eth1/57/1		Eth1/56/3,
Eth1/57/3, Eth1/57/4		Eth1/57/2,
Eth1/58/2, Eth1/58/3		Eth1/58/1,
Eth1/59/1, Eth1/59/2		Eth1/58/4,
Eth1/59/4, Eth1/60/1		Eth1/59/3,
Eth1/60/3, Eth1/60/4		Eth1/60/2,
Eth1/61/2, Eth1/61/3		Eth1/61/1,
Eth1/62/1, Eth1/62/2		Eth1/61/4,
40 VLAN0040	active	Eth1/62/3, Eth1/62/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
Eth1/2/2		Eth1/1/4, Eth1/2/1,
Eth1/3/1		Eth1/2/3, Eth1/2/4,
Eth1/3/4		Eth1/3/2, Eth1/3/3,
Eth1/4/3		Eth1/4/1, Eth1/4/2,
Eth1/5/2		Eth1/4/4, Eth1/5/1,
Eth1/6/1		Eth1/5/3, Eth1/5/4,
Eth1/6/4		Eth1/6/2, Eth1/6/3,
Eth1/7/3		Eth1/7/1, Eth1/7/2,
		Eth1/7/4, Eth1/8/1,

Eth1/8/2

Eth1/9/1

Eth1/9/4

Eth1/10/2, Eth1/10/3

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/8/3, Eth1/8/4,

Eth1/9/2, Eth1/9/3,

Eth1/10/1,

Eth1/10/4,

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/31/2, Eth1/31/3

Eth1/32/1, Eth1/32/2

Eth1/32/4, Eth1/33/1

Eth1/33/3, Eth1/33/4

Eth1/34/2, Eth1/34/3

Eth1/35/1, Eth1/35/2

Eth1/35/4, Eth1/36/1

Eth1/36/3, Eth1/36/4

Eth1/37/2, Eth1/37/3

Eth1/38/1, Eth1/38/2

Eth1/38/4, Eth1/39/1

Eth1/39/3, Eth1/39/4

Eth1/40/2, Eth1/40/3

Eth1/41/1, Eth1/41/2

Eth1/41/4, Eth1/42/1

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

Eth1/31/1,

Eth1/31/4,

Eth1/32/3,

Eth1/33/2,

Eth1/34/1,

Eth1/34/4,

Eth1/35/3,

Eth1/36/2,

Eth1/37/1,

Eth1/37/4,

Eth1/38/3,

Eth1/39/2,

Eth1/40/1,

Eth1/40/4,

Eth1/41/3,

Eth1/42/2,

Eth1/42/3, Eth1/42/4

Eth1/43/2, Eth1/43/3

Eth1/44/1, Eth1/44/2

Eth1/44/4, Eth1/45/1

Eth1/45/3, Eth1/45/4

Eth1/46/2, Eth1/46/3

Eth1/47/1, Eth1/47/2

Eth1/47/4, Eth1/48/1

Eth1/48/3, Eth1/48/4

Eth1/49/2, Eth1/49/3

Eth1/50/1, Eth1/50/2

Eth1/50/4, Eth1/51/1

Eth1/51/3, Eth1/51/4

Eth1/52/2, Eth1/52/3

Eth1/53/1, Eth1/53/2

Eth1/53/4, Eth1/54/1

Eth1/54/3, Eth1/54/4

Eth1/55/2, Eth1/55/3

Eth1/56/1, Eth1/56/2

Eth1/56/4, Eth1/57/1

Eth1/57/3, Eth1/57/4

Eth1/58/2, Eth1/58/3

Eth1/59/1, Eth1/59/2

Eth1/43/1,

Eth1/43/4,

Eth1/44/3,

Eth1/45/2,

Eth1/46/1,

Eth1/46/4,

Eth1/47/3,

Eth1/48/2,

Eth1/49/1,

Eth1/49/4,

Eth1/50/3,

Eth1/51/2,

Eth1/52/1,

Eth1/52/4,

Eth1/53/3,

Eth1/54/2,

Eth1/55/1,

Eth1/55/4,

Eth1/56/3,

Eth1/57/2,

Eth1/58/1,

Eth1/58/4,

Eth1/59/3,

Eth1/59/4, Eth1/60/1

Eth1/60/2,

Eth1/60/3, Eth1/60/4

Eth1/61/1,

Eth1/61/2, Eth1/61/3

Eth1/61/4,

Eth1/62/1, Eth1/62/2

Eth1/62/3, Eth1/62/4

cs1# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1/1	1	trunking	--
Eth1/1/2	1	trunking	--
Eth1/1/3	1	trunking	--
Eth1/1/4	1	trunking	--
Eth1/2/1	1	trunking	--
Eth1/2/2	1	trunking	--
Eth1/2/3	1	trunking	--
Eth1/2/4	1	trunking	--
.			
.			
.			
Eth1/62/2	none		
Eth1/62/3	none		
Eth1/62/4	none		
Eth1/63	none		
Eth1/64	none		
Pol	1		



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

3. 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      Eth1/63 (P)  Eth1/64 (P)
999    Po999 (SD)    Eth      NONE      --
cs1#
```

Paso 3: Configure el cluster ONTAP

NetApp recomienda usar System Manager para configurar clústeres nuevos.

System Manager proporciona un flujo de trabajo sencillo y sencillo para la instalación y la configuración del clúster, incluidas la asignación de una dirección IP de gestión de nodos, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento del almacenamiento inicial.

Vaya a ["Configure ONTAP en un nuevo clúster con System Manager"](#) para obtener instrucciones de configuración.

El futuro

Después de haber instalado el RCF, ["verificar la configuración de SSH"](#) .

Actualice su archivo de configuración de referencia (RCF)

Actualice la versión de RCF cuando tenga instalada una versión existente del archivo RCF en los conmutadores operativos.

Antes de empezar

Asegúrese de tener lo siguiente:

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El RCF actual.

- Si está actualizando la versión de RCF, necesita una configuración de inicio en el RCF que refleje las imágenes de inicio deseadas.

Si necesita cambiar la configuración 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.



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.



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

Paso 1: Prepárese para la actualización

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.

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

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

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

```
network device-discovery show
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1-01/cdp
          e10a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/3  N9K-
C9364D-GX2A
          e10b   cs1 (FDOXXXXXXXXXX)      Ethernet1/13/3  N9K-
C9364D-GX2A
          e11a   cs1 (FLMXXXXXXXXXX)      Ethernet1/16/4  N9K-
C9364D-GX2A
          e11b   cs1 (FDOXXXXXXXXXX)      Ethernet1/13/4  N9K-
C9364D-GX2A
          e1a    cs1 (FLMXXXXXXXXXX)      Ethernet1/16/1  N9K-
C9364D-GX2A
          e1b    cs1 (FDOXXXXXXXXXX)      Ethernet1/13/1  N9K-
C9364D-GX2A
          .
          .
          .
          e7a    cs1 (FLMXXXXXXXXXX)      Ethernet1/16/2  N9K-
C9364D-GX2A
          e7b    cs1 (FDOXXXXXXXXXX)      Ethernet1/13/2  N9K-
C9364D-GX2A
node1-01/lldp
          e10a   cs1 (c8:60:8f:xx:xx:xx)  Ethernet1/16/3  -
          e10b   cs2 (04:e3:87:xx:xx:xx)  Ethernet1/16/3  -
          e11a   cs1 (c8:60:8f:xx:xx:xx)  Ethernet1/16/4  -
          e11b   cs2 (04:e3:87:xx:xx:xx)  Ethernet1/16/4  -
          e1a    cs1 (c8:60:8f:xx:xx:xx)  Ethernet1/16/1  -
          e1b    cs2 (04:e3:87:xx:xx:xx)  Ethernet1/16/1  -
          .
          .
          .
          e7a    cs1 (c8:60:8f:xx:xx:xx)  Ethernet1/16/2  -
          e7b    cs2 (04:e3:87:xx:xx:xx)  Ethernet1/16/2  -
          .
          .
          .
```


4. Consulta el estado administrativo y operativo de cada puerto.

a. **Puertos de clúster**

i. 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: node1-01

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node:node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

cluster1::*>

- ii. 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
```

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

Cluster			
	node1-01_clus1	up/up	169.254.3.4/23
node1-01	e7a true		
	node1-01_clus2	up/up	169.254.3.5/23
node1-01	e7b true		
	node1-02_clus1	up/up	169.254.3.8/23
node1-02	e7a true		
	node1-02_clus2	up/up	169.254.3.9/23
node1-02	e7b true		
	node1-03_clus1	up/up	169.254.1.3/23
node1-03	e7a true		
	node1-03_clus2	up/up	169.254.1.1/23
node1-03	e7b true		
	node1-04_clus1	up/up	169.254.1.6/23
node1-04	e7a true		
	node1-04_clus2	up/up	169.254.1.7/23
node1-04	e7b true		
8 entries were displayed.			

iii. Verifique que el clúster muestre información para ambos conmutadores:

```
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 (FDOXXXXXXXX)                         cluster-network                    10.228.137.233
N9K-C9364D-GX2A
    Serial Number: FDOXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP

cs2 (FLMXXXXXXXX)                         cluster-network                    10.228.137.234
N9K-C9364D-GX2A
    Serial Number: FLMXXXXXXXX
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                10.4(2)
    Version Source: CDP/ISDP
```

b. Puertos HA

- i. Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf ID	Module	State	Internal?
1.1			
0	A	connected	false
1	A	connected	false
2	A	connected	false
3	A	connected	false
4	A	connected	false
5	A	connected	false
6	A	connected	false
7	A	connected	false
8	B	connected	false
9	B	connected	false
10	B	connected	false
11	B	connected	false
12	B	connected	false
13	B	connected	false
14	B	connected	false
15	B	connected	false

```
16 entries were displayed.
```

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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


Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

5. Deshabilite la reversión automática en las LIF del clúster:

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

Paso 2: Configurar puertos

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

```

cs1# config
cs1(config)# interface e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-
4,e1/6/1-4,e1/7/1-4,e1/8/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/9/1-4,e1/10/1-4,e1/11/1-4,e1/12/1-4,e1/13/1-
4,e1/14/1-4,e1/15/1-4,e1/16/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/17/1-4,e1/18/1-4,e1/19/1-4,e1/20/1-4,e1/21/1-
4,e1/22/1-4,e1/23/1-4,e1/24/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/25/1-4,e1/26/1-4,e1/27/1-4,e1/28/1-4,e1/29/1-
4,e1/30/1-4,e1/31/1-4,e1/32/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/33/1-4,e1/34/1-4,e1/35/1-4,e1/36/1-4,e1/37/1-
4,e1/38/1-4,e1/39/1-4,e1/40/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/41/1-4,e1/42/1-4,e1/43/1-4,e1/44/1-4,e1/35/1-
4,e1/46/1-4,e1/47/1-4,e1/48/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/49/1-4,e1/50/1-4,e1/51/1-4,e1/52/1-4,e1/53/1-
4,e1/54/1-4,e1/55/1-4,e1/56/1-4
cs1(config-if-range)# shutdown
cs1(config)# interface e1/57/1-4,e1/58/1-4,e1/59/1-4,e1/60/1-4,e1/61/1-
4,e1/62/1-4
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit

```



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

2. Compruebe que las LIF del clúster han conmutado al nodo de respaldo a los puertos alojados en el switch del clúster CS1. 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				
	node1-01_clus1	up/up	169.254.36.44/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.7.5/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.197.206/16	node1-02
e7a	true			
	node1-02_clus2	up/up	169.254.195.186/16	node1-02
e7b	true			
	node1-03_clus1	up/up	169.254.192.49/16	node1-03
e7a	true			
	node1-03_clus2	up/up	169.254.182.76/16	node1-03
e7b	true			
	node1-04_clus1	up/up	169.254.59.49/16	node1-04
e7a	true			
	node1-04_clus2	up/up	169.254.62.244/16	node1-04
e7b	true			

8 entries were displayed.

3. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

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

```
show running-config
```

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



Asegúrese de configurar lo siguiente:

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

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

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

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

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

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

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

```
cs1# echo "hardware access-list tcam region ing-l2-qos 1536" >>  
bootflash:write_erase.cfg
```

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

6. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

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

7. Emitir el `write erase` Comando para borrar la configuración guardada actual:

```
cs1# write erase
```

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

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

8. Copie la configuración básica guardada anteriormente en la configuración de inicio.

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

9. Reinicie el switch:

```
cs1# reload
```

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

10. Cuando se pueda volver a acceder a la dirección IP de administración, inicie sesión en el switch a través de SSH.

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

11. Copie el RCF al bootflash del switch CS1 usando 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 9000"](#) guías.

Muestra el ejemplo

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: NX9364D-GX2A-RCF-v10.0-Shared.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)...
```

12. 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 9000"](#) guías.

Este ejemplo muestra el archivo RCF NX9364D-GX2A-RCF-v10.0-Shared.txt siendo instalado en el switch cs1:

```
cs1# copy NX9364D-GX2A-RCF-v10.0-Shared.txt running-config echo-commands
```



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

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. Vuelva a aplicar cualquier personalización anterior a la configuración del conmutador.
15. Después de comprobar que las versiones de RCF, las adiciones personalizadas y la configuración del switch son correctas, 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 9000"](#) guías.

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

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

16. Reinicie el interruptor CS1. Puede ignorar las alertas de «monitor de estado del switch del clúster» y los eventos de «puertos inactivos» que se notifican en los nodos mientras se reinicia el switch.

```
cs1# reload
```

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

17. Verificar el estado de los puertos en el clúster.

a. Puertos de clúster

- i. Compruebe que los puertos del clúster estén en buen estado en todos los nodos del clúster:

```
network port show -ip space Cluster
```

Muestra el ejemplo

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

Node: node1-01

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-02

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node1-03

Ignore

						Speed(Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
-----	-----					
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node1-04

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e7b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

8 entries were displayed.

ii. Compruebe el estado del switch del clúster.

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

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


Muestra el ejemplo

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

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

node1-01/cdp			
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3
N9K-C9364D-GX2A			
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/3
N9K-C9364D-GX2A			
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4
N9K-C9364D-GX2A			
	e11b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/4
N9K-C9364D-GX2A			
	e1a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/1
N9K-C9364D-GX2A			
	e1b	cs2 (FLMXXXXXXXXX)	Ethernet1/13/1
N9K-C9364D-GX2A			
	.		
	.		
	.		
	e7a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/2
N9K-C9364D-GX2A			
	e7b	cs2 (FDOXXXXXXXXX)	Ethernet1/13/2
N9K-C9364D-GX2A			
node1-02/cdp			
	.		
	.		
	.		

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

Switch Model	Type	Address

cs2 (FDOXXXXXXXXX) N9K-C9364D-GX2A	cluster-network	10.228.137.233
Serial Number: FDOXXXXXXXXX		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		

```
10.4(2)
Version Source: CDP/ISDP

cs1 (FLMXXXXXXXXX)          cluster-network    10.228.137.234
N9K-C9364D-GX2A
  Serial Number: FLMXXXXXXXXX
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
10.4(2)
Version Source: CDP/ISDP

2 entries were displayed.
```

b. Puertos HA

- i. Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: e1a-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: e1b-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: e1a-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04						
	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

16 entries were displayed.

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

16 entries were displayed.

18. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

19. Repita los pasos 4 a 18 en el interruptor cs2.

20. Habilite la reversión automática en las LIF del clúster:

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

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

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

```
show interface brief
```

Muestra el ejemplo

```
cs1# show interface brief | grep up
.
.
Eth1/9/3          1      eth  trunk  up      none
100G(D) --
Eth1/9/4          1      eth  trunk  up      none
100G(D) --
Eth1/15/1         1      eth  trunk  up      none
100G(D) --
Eth1/15/2         1      eth  trunk  up      none
100G(D) --
Eth1/15/3         1      eth  trunk  up      none
100G(D) --
Eth1/15/4         1      eth  trunk  up      none
100G(D) --
Eth1/16/1         1      eth  trunk  up      none
100G(D) --
Eth1/16/2         1      eth  trunk  up      none
100G(D) --
Eth1/16/3         1      eth  trunk  up      none
100G(D) --
Eth1/16/4         1      eth  trunk  up      none
100G(D) --
Eth1/17/1         1      eth  trunk  up      none
100G(D) --
Eth1/17/2         1      eth  trunk  up      none
100G(D) --
Eth1/17/3         1      eth  trunk  up      none
100G(D) --
Eth1/17/4         1      eth  trunk  up      none
100G(D) --
.
.
.
```

2. Compruebe que los nodos esperados siguen conectados:

```
show cdp neighbors
```


Muestra el ejemplo

```
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
cs2 (FDOXXXXXXXXX) Eth1/31	Eth1/63	179	R S I s	N9K-C9332D-GX2B
cs2 (FDOXXXXXXXXX) Eth1/32	Eth1/64	179	R S I s	N9K-C9332D-GX2B
node1-01 e1a	Eth1/4/1	123	H	AFX-1K
node1-01 e7a	Eth1/4/2	123	H	AFX-1K
node1-01 e10a	Eth1/4/3	123	H	AFX-1K
node1-01 e11a	Eth1/4/4	123	H	AFX-1K
node1-02 e1a	Eth1/9/1	138	H	AFX-1K
node1-02 e7a	Eth1/9/2	138	H	AFX-1K
node1-02 e10a	Eth1/9/3	138	H	AFX-1K
node1-02 e11a	Eth1/9/4	138	H	AFX-1K
node1-03 e1a	Eth1/15/1	138	H	AFX-1K
node1-03 e7a	Eth1/15/2	138	H	AFX-1K
node1-03 e10a	Eth1/15/3	138	H	AFX-1K
node1-03 e11a	Eth1/15/4	138	H	AFX-1K
node1-04 e1a	Eth1/16/1	173	H	AFX-1K
node1-04 e7a	Eth1/16/2	173	H	AFX-1K
node1-04 e10a	Eth1/16/3	173	H	AFX-1K

```
node1-04          Eth1/16/4      173    H      AFX-1K
e11a
```

```
Total entries displayed: 18
```

3. Compruebe que los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Po999, Eth1/63, Eth1/64 Eth1/65, Eth1/66, Eth1/1/1 Eth1/1/2, Eth1/1/3, Eth1/1/4 Eth1/2/1, Eth1/2/2, Eth1/2/3 Eth1/2/4, Eth1/3/1, Eth1/3/2 Eth1/3/3, Eth1/3/4, Eth1/4/1 Eth1/4/2, Eth1/4/3, Eth1/4/4 Eth1/5/1, Eth1/5/2, Eth1/5/3 Eth1/5/4, Eth1/6/1, Eth1/6/2 Eth1/6/3, Eth1/6/4, Eth1/7/1 Eth1/7/2, Eth1/7/3, Eth1/7/4 Eth1/8/1, Eth1/8/2, Eth1/8/3 Eth1/8/4, Eth1/9/1, Eth1/9/2 Eth1/9/3, Eth1/9/4, Eth1/10/1 Eth1/10/2, Eth1/10/3, Eth1/10/4 Eth1/11/1, Eth1/11/2, Eth1/11/3 Eth1/11/4, Eth1/12/1, Eth1/12/2 Eth1/12/3, Eth1/12/4, Eth1/13/1 Eth1/13/2, Eth1/13/3, Eth1/13/4 Eth1/14/1,

Eth1/14/2, Eth1/14/3

Eth1/15/1, Eth1/15/2

Eth1/15/4, Eth1/16/1

Eth1/16/3, Eth1/16/4

Eth1/17/2, Eth1/17/3

Eth1/18/1, Eth1/18/2

Eth1/18/4, Eth1/19/1

Eth1/19/3, Eth1/19/4

Eth1/20/2, Eth1/20/3

Eth1/21/1, Eth1/21/2

Eth1/21/4, Eth1/22/1

Eth1/22/3, Eth1/22/4

Eth1/23/2, Eth1/23/3

Eth1/24/1, Eth1/24/2

Eth1/24/4, Eth1/25/1

Eth1/25/3, Eth1/25/4

Eth1/26/2, Eth1/26/3

Eth1/27/1, Eth1/27/2

Eth1/27/4, Eth1/28/1

Eth1/28/3, Eth1/28/4

Eth1/29/2, Eth1/29/3

Eth1/30/1, Eth1/30/2

Eth1/30/4, Eth1/31/1

Eth1/14/4,

Eth1/15/3,

Eth1/16/2,

Eth1/17/1,

Eth1/17/4,

Eth1/18/3,

Eth1/19/2,

Eth1/20/1,

Eth1/20/4,

Eth1/21/3,

Eth1/22/2,

Eth1/23/1,

Eth1/23/4,

Eth1/24/3,

Eth1/25/2,

Eth1/26/1,

Eth1/26/4,

Eth1/27/3,

Eth1/28/2,

Eth1/29/1,

Eth1/29/4,

Eth1/30/3,

Eth1/31/2,

Eth1/31/3, Eth1/31/4

Eth1/32/2, Eth1/32/3

Eth1/33/1, Eth1/33/2

Eth1/33/4, Eth1/34/1

Eth1/34/3, Eth1/34/4

Eth1/35/2, Eth1/35/3

Eth1/36/1, Eth1/36/2

Eth1/36/4, Eth1/37/1

Eth1/37/3, Eth1/37/4

Eth1/38/2, Eth1/38/3

Eth1/39/1, Eth1/39/2

Eth1/39/4, Eth1/40/1

Eth1/40/3, Eth1/40/4

Eth1/41/2, Eth1/41/3

Eth1/42/1, Eth1/42/2

Eth1/42/4, Eth1/43/1

Eth1/43/3, Eth1/43/4

Eth1/44/2, Eth1/44/3

Eth1/45/1, Eth1/45/2

Eth1/45/4, Eth1/46/1

Eth1/46/3, Eth1/46/4

Eth1/47/2, Eth1/47/3

Eth1/48/1, Eth1/48/2

Eth1/32/1,

Eth1/32/4,

Eth1/33/3,

Eth1/34/2,

Eth1/35/1,

Eth1/35/4,

Eth1/36/3,

Eth1/37/2,

Eth1/38/1,

Eth1/38/4,

Eth1/39/3,

Eth1/40/2,

Eth1/41/1,

Eth1/41/4,

Eth1/42/3,

Eth1/43/2,

Eth1/44/1,

Eth1/44/4,

Eth1/45/3,

Eth1/46/2,

Eth1/47/1,

Eth1/47/4,

Eth1/48/3,

Eth1/48/4, Eth1/49/1		Eth1/49/2,
Eth1/49/3, Eth1/49/4		Eth1/50/1,
Eth1/50/2, Eth1/50/3		Eth1/50/4,
Eth1/51/1, Eth1/51/2		Eth1/51/3,
Eth1/51/4, Eth1/52/1		Eth1/52/2,
Eth1/52/3, Eth1/52/4		Eth1/53/1,
Eth1/53/2, Eth1/53/3		Eth1/53/4,
Eth1/54/1, Eth1/54/2		Eth1/54/3,
Eth1/54/4, Eth1/55/1		Eth1/55/2,
Eth1/55/3, Eth1/55/4		Eth1/56/1,
Eth1/56/2, Eth1/56/3		Eth1/56/4,
Eth1/57/1, Eth1/57/2		Eth1/57/3,
Eth1/57/4, Eth1/58/1		Eth1/58/2,
Eth1/58/3, Eth1/58/4		Eth1/59/1,
Eth1/59/2, Eth1/59/3		Eth1/59/4,
Eth1/60/1, Eth1/60/2		Eth1/60/3,
Eth1/60/4, Eth1/61/1		Eth1/61/2,
Eth1/61/3, Eth1/61/4		Eth1/62/1,
Eth1/62/2, Eth1/62/3		Eth1/62/4
17 VLAN0017	active	Eth1/1/1, Eth1/1/2,
Eth1/1/3		Eth1/1/4, Eth1/2/1,
Eth1/2/2		Eth1/2/3, Eth1/2/4,
Eth1/3/1		Eth1/3/2, Eth1/3/3,
Eth1/3/4		

Eth1/4/3	Eth1/4/1, Eth1/4/2,
Eth1/5/2	Eth1/4/4, Eth1/5/1,
Eth1/6/1	Eth1/5/3, Eth1/5/4,
Eth1/6/4	Eth1/6/2, Eth1/6/3,
Eth1/7/3	Eth1/7/1, Eth1/7/2,
Eth1/8/2	Eth1/7/4, Eth1/8/1,
Eth1/9/1	Eth1/8/3, Eth1/8/4,
Eth1/9/4	Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3	Eth1/10/1,
Eth1/11/1, Eth1/11/2	Eth1/10/4,
Eth1/11/4, Eth1/12/1	Eth1/11/3,
Eth1/12/3, Eth1/12/4	Eth1/12/2,
Eth1/13/2, Eth1/13/3	Eth1/13/1,
Eth1/14/1, Eth1/14/2	Eth1/13/4,
Eth1/14/4, Eth1/15/1	Eth1/14/3,
Eth1/15/3, Eth1/15/4	Eth1/15/2,
Eth1/16/2, Eth1/16/3	Eth1/16/1,
Eth1/17/1, Eth1/17/2	Eth1/16/4,
Eth1/17/4, Eth1/18/1	Eth1/17/3,
Eth1/18/3, Eth1/18/4	Eth1/18/2,
Eth1/19/2, Eth1/19/3	Eth1/19/1,
Eth1/20/1, Eth1/20/2	Eth1/19/4,
Eth1/20/4, Eth1/21/1	Eth1/20/3,

Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4
Eth1/31/2, Eth1/31/3
Eth1/32/1, Eth1/32/2
Eth1/32/4, Eth1/33/1
Eth1/33/3, Eth1/33/4
Eth1/34/2, Eth1/34/3
Eth1/35/1, Eth1/35/2
Eth1/35/4, Eth1/36/1
Eth1/36/3, Eth1/36/4
Eth1/37/2, Eth1/37/3
Eth1/38/1, Eth1/38/2

Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,
Eth1/31/1,
Eth1/31/4,
Eth1/32/3,
Eth1/33/2,
Eth1/34/1,
Eth1/34/4,
Eth1/35/3,
Eth1/36/2,
Eth1/37/1,
Eth1/37/4,

Eth1/38/4, Eth1/39/1
Eth1/39/3, Eth1/39/4
Eth1/40/2, Eth1/40/3
Eth1/41/1, Eth1/41/2
Eth1/41/4, Eth1/42/1
Eth1/42/3, Eth1/42/4
Eth1/43/2, Eth1/43/3
Eth1/44/1, Eth1/44/2
Eth1/44/4, Eth1/45/1
Eth1/45/3, Eth1/45/4
Eth1/46/2, Eth1/46/3
Eth1/47/1, Eth1/47/2
Eth1/47/4, Eth1/48/1
Eth1/48/3, Eth1/48/4
Eth1/49/2, Eth1/49/3
Eth1/50/1, Eth1/50/2
Eth1/50/4, Eth1/51/1
Eth1/51/3, Eth1/51/4
Eth1/52/2, Eth1/52/3
Eth1/53/1, Eth1/53/2
Eth1/53/4, Eth1/54/1
Eth1/54/3, Eth1/54/4
Eth1/55/2, Eth1/55/3

Eth1/38/3,
Eth1/39/2,
Eth1/40/1,
Eth1/40/4,
Eth1/41/3,
Eth1/42/2,
Eth1/43/1,
Eth1/43/4,
Eth1/44/3,
Eth1/45/2,
Eth1/46/1,
Eth1/46/4,
Eth1/47/3,
Eth1/48/2,
Eth1/49/1,
Eth1/49/4,
Eth1/50/3,
Eth1/51/2,
Eth1/52/1,
Eth1/52/4,
Eth1/53/3,
Eth1/54/2,
Eth1/55/1,

Eth1/56/1, Eth1/56/2		Eth1/55/4,
Eth1/56/4, Eth1/57/1		Eth1/56/3,
Eth1/57/3, Eth1/57/4		Eth1/57/2,
Eth1/58/2, Eth1/58/3		Eth1/58/1,
Eth1/59/1, Eth1/59/2		Eth1/58/4,
Eth1/59/4, Eth1/60/1		Eth1/59/3,
Eth1/60/3, Eth1/60/4		Eth1/60/2,
Eth1/61/2, Eth1/61/3		Eth1/61/1,
Eth1/62/1, Eth1/62/2		Eth1/61/4,
18 VLAN0018	active	Eth1/62/3, Eth1/62/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
Eth1/2/2		Eth1/1/4, Eth1/2/1,
Eth1/3/1		Eth1/2/3, Eth1/2/4,
Eth1/3/4		Eth1/3/2, Eth1/3/3,
Eth1/4/3		Eth1/4/1, Eth1/4/2,
Eth1/5/2		Eth1/4/4, Eth1/5/1,
Eth1/6/1		Eth1/5/3, Eth1/5/4,
Eth1/6/4		Eth1/6/2, Eth1/6/3,
Eth1/7/3		Eth1/7/1, Eth1/7/2,
Eth1/8/2		Eth1/7/4, Eth1/8/1,
Eth1/9/1		Eth1/8/3, Eth1/8/4,
Eth1/9/4		Eth1/9/2, Eth1/9/3,
Eth1/10/2, Eth1/10/3		Eth1/10/1,
		Eth1/10/4,

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/31/2, Eth1/31/3

Eth1/32/1, Eth1/32/2

Eth1/32/4, Eth1/33/1

Eth1/33/3, Eth1/33/4

Eth1/34/2, Eth1/34/3

Eth1/35/1, Eth1/35/2

Eth1/35/4, Eth1/36/1

Eth1/36/3, Eth1/36/4

Eth1/37/2, Eth1/37/3

Eth1/38/1, Eth1/38/2

Eth1/38/4, Eth1/39/1

Eth1/39/3, Eth1/39/4

Eth1/40/2, Eth1/40/3

Eth1/41/1, Eth1/41/2

Eth1/41/4, Eth1/42/1

Eth1/42/3, Eth1/42/4

Eth1/43/2, Eth1/43/3

Eth1/44/1, Eth1/44/2

Eth1/44/4, Eth1/45/1

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

Eth1/31/1,

Eth1/31/4,

Eth1/32/3,

Eth1/33/2,

Eth1/34/1,

Eth1/34/4,

Eth1/35/3,

Eth1/36/2,

Eth1/37/1,

Eth1/37/4,

Eth1/38/3,

Eth1/39/2,

Eth1/40/1,

Eth1/40/4,

Eth1/41/3,

Eth1/42/2,

Eth1/43/1,

Eth1/43/4,

Eth1/44/3,

Eth1/45/2,

Eth1/45/3, Eth1/45/4

Eth1/46/2, Eth1/46/3

Eth1/47/1, Eth1/47/2

Eth1/47/4, Eth1/48/1

Eth1/48/3, Eth1/48/4

Eth1/49/2, Eth1/49/3

Eth1/50/1, Eth1/50/2

Eth1/50/4, Eth1/51/1

Eth1/51/3, Eth1/51/4

Eth1/52/2, Eth1/52/3

Eth1/53/1, Eth1/53/2

Eth1/53/4, Eth1/54/1

Eth1/54/3, Eth1/54/4

Eth1/55/2, Eth1/55/3

Eth1/56/1, Eth1/56/2

Eth1/56/4, Eth1/57/1

Eth1/57/3, Eth1/57/4

Eth1/58/2, Eth1/58/3

Eth1/59/1, Eth1/59/2

Eth1/59/4, Eth1/60/1

Eth1/60/3, Eth1/60/4

Eth1/61/2, Eth1/61/3

Eth1/62/1, Eth1/62/2

Eth1/46/1,

Eth1/46/4,

Eth1/47/3,

Eth1/48/2,

Eth1/49/1,

Eth1/49/4,

Eth1/50/3,

Eth1/51/2,

Eth1/52/1,

Eth1/52/4,

Eth1/53/3,

Eth1/54/2,

Eth1/55/1,

Eth1/55/4,

Eth1/56/3,

Eth1/57/2,

Eth1/58/1,

Eth1/58/4,

Eth1/59/3,

Eth1/60/2,

Eth1/61/1,

Eth1/61/4,

Eth1/62/3, Eth1/62/4

30	VLAN0030	active	Eth1/1/1, Eth1/1/2,
	Eth1/1/3		Eth1/1/4, Eth1/2/1,
	Eth1/2/2		Eth1/2/3, Eth1/2/4,
	Eth1/3/1		Eth1/3/2, Eth1/3/3,
	Eth1/3/4		Eth1/4/1, Eth1/4/2,
	Eth1/4/3		Eth1/4/4, Eth1/5/1,
	Eth1/5/2		Eth1/5/3, Eth1/5/4,
	Eth1/6/1		Eth1/6/2, Eth1/6/3,
	Eth1/6/4		Eth1/7/1, Eth1/7/2,
	Eth1/7/3		Eth1/7/4, Eth1/8/1,
	Eth1/8/2		Eth1/8/3, Eth1/8/4,
	Eth1/9/1		Eth1/9/2, Eth1/9/3,
	Eth1/9/4		Eth1/10/1,
	Eth1/10/2, Eth1/10/3		Eth1/10/4,
	Eth1/11/1, Eth1/11/2		Eth1/11/3,
	Eth1/11/4, Eth1/12/1		Eth1/12/2,
	Eth1/12/3, Eth1/12/4		Eth1/13/1,
	Eth1/13/2, Eth1/13/3		Eth1/13/4,
	Eth1/14/1, Eth1/14/2		Eth1/14/3,
	Eth1/14/4, Eth1/15/1		Eth1/15/2,
	Eth1/15/3, Eth1/15/4		Eth1/16/1,
	Eth1/16/2, Eth1/16/3		Eth1/16/4,
	Eth1/17/1, Eth1/17/2		Eth1/17/3,
	Eth1/17/4, Eth1/18/1		

Eth1/18/3, Eth1/18/4
Eth1/19/2, Eth1/19/3
Eth1/20/1, Eth1/20/2
Eth1/20/4, Eth1/21/1
Eth1/21/3, Eth1/21/4
Eth1/22/2, Eth1/22/3
Eth1/23/1, Eth1/23/2
Eth1/23/4, Eth1/24/1
Eth1/24/3, Eth1/24/4
Eth1/25/2, Eth1/25/3
Eth1/26/1, Eth1/26/2
Eth1/26/4, Eth1/27/1
Eth1/27/3, Eth1/27/4
Eth1/28/2, Eth1/28/3
Eth1/29/1, Eth1/29/2
Eth1/29/4, Eth1/30/1
Eth1/30/3, Eth1/30/4
Eth1/31/2, Eth1/31/3
Eth1/32/1, Eth1/32/2
Eth1/32/4, Eth1/33/1
Eth1/33/3, Eth1/33/4
Eth1/34/2, Eth1/34/3
Eth1/35/1, Eth1/35/2

Eth1/18/2,
Eth1/19/1,
Eth1/19/4,
Eth1/20/3,
Eth1/21/2,
Eth1/22/1,
Eth1/22/4,
Eth1/23/3,
Eth1/24/2,
Eth1/25/1,
Eth1/25/4,
Eth1/26/3,
Eth1/27/2,
Eth1/28/1,
Eth1/28/4,
Eth1/29/3,
Eth1/30/2,
Eth1/31/1,
Eth1/31/4,
Eth1/32/3,
Eth1/33/2,
Eth1/34/1,
Eth1/34/4,

Eth1/35/4, Eth1/36/1
Eth1/36/3, Eth1/36/4
Eth1/37/2, Eth1/37/3
Eth1/38/1, Eth1/38/2
Eth1/38/4, Eth1/39/1
Eth1/39/3, Eth1/39/4
Eth1/40/2, Eth1/40/3
Eth1/41/1, Eth1/41/2
Eth1/41/4, Eth1/42/1
Eth1/42/3, Eth1/42/4
Eth1/43/2, Eth1/43/3
Eth1/44/1, Eth1/44/2
Eth1/44/4, Eth1/45/1
Eth1/45/3, Eth1/45/4
Eth1/46/2, Eth1/46/3
Eth1/47/1, Eth1/47/2
Eth1/47/4, Eth1/48/1
Eth1/48/3, Eth1/48/4
Eth1/49/2, Eth1/49/3
Eth1/50/1, Eth1/50/2
Eth1/50/4, Eth1/51/1
Eth1/51/3, Eth1/51/4
Eth1/52/2, Eth1/52/3

Eth1/35/3,
Eth1/36/2,
Eth1/37/1,
Eth1/37/4,
Eth1/38/3,
Eth1/39/2,
Eth1/40/1,
Eth1/40/4,
Eth1/41/3,
Eth1/42/2,
Eth1/43/1,
Eth1/43/4,
Eth1/44/3,
Eth1/45/2,
Eth1/46/1,
Eth1/46/4,
Eth1/47/3,
Eth1/48/2,
Eth1/49/1,
Eth1/49/4,
Eth1/50/3,
Eth1/51/2,
Eth1/52/1,

Eth1/53/1, Eth1/53/2		Eth1/52/4,
Eth1/53/4, Eth1/54/1		Eth1/53/3,
Eth1/54/3, Eth1/54/4		Eth1/54/2,
Eth1/55/2, Eth1/55/3		Eth1/55/1,
Eth1/56/1, Eth1/56/2		Eth1/55/4,
Eth1/56/4, Eth1/57/1		Eth1/56/3,
Eth1/57/3, Eth1/57/4		Eth1/57/2,
Eth1/58/2, Eth1/58/3		Eth1/58/1,
Eth1/59/1, Eth1/59/2		Eth1/58/4,
Eth1/59/4, Eth1/60/1		Eth1/59/3,
Eth1/60/3, Eth1/60/4		Eth1/60/2,
Eth1/61/2, Eth1/61/3		Eth1/61/1,
Eth1/62/1, Eth1/62/2		Eth1/61/4,
40 VLAN0040	active	Eth1/62/3, Eth1/62/4
Eth1/1/3		Eth1/1/1, Eth1/1/2,
Eth1/2/2		Eth1/1/4, Eth1/2/1,
Eth1/3/1		Eth1/2/3, Eth1/2/4,
Eth1/3/4		Eth1/3/2, Eth1/3/3,
Eth1/4/3		Eth1/4/1, Eth1/4/2,
Eth1/5/2		Eth1/4/4, Eth1/5/1,
Eth1/6/1		Eth1/5/3, Eth1/5/4,
Eth1/6/4		Eth1/6/2, Eth1/6/3,
Eth1/7/3		Eth1/7/1, Eth1/7/2,
		Eth1/7/4, Eth1/8/1,

Eth1/8/2

Eth1/9/1

Eth1/9/4

Eth1/10/2, Eth1/10/3

Eth1/11/1, Eth1/11/2

Eth1/11/4, Eth1/12/1

Eth1/12/3, Eth1/12/4

Eth1/13/2, Eth1/13/3

Eth1/14/1, Eth1/14/2

Eth1/14/4, Eth1/15/1

Eth1/15/3, Eth1/15/4

Eth1/16/2, Eth1/16/3

Eth1/17/1, Eth1/17/2

Eth1/17/4, Eth1/18/1

Eth1/18/3, Eth1/18/4

Eth1/19/2, Eth1/19/3

Eth1/20/1, Eth1/20/2

Eth1/20/4, Eth1/21/1

Eth1/21/3, Eth1/21/4

Eth1/22/2, Eth1/22/3

Eth1/23/1, Eth1/23/2

Eth1/23/4, Eth1/24/1

Eth1/24/3, Eth1/24/4

Eth1/8/3, Eth1/8/4,

Eth1/9/2, Eth1/9/3,

Eth1/10/1,

Eth1/10/4,

Eth1/11/3,

Eth1/12/2,

Eth1/13/1,

Eth1/13/4,

Eth1/14/3,

Eth1/15/2,

Eth1/16/1,

Eth1/16/4,

Eth1/17/3,

Eth1/18/2,

Eth1/19/1,

Eth1/19/4,

Eth1/20/3,

Eth1/21/2,

Eth1/22/1,

Eth1/22/4,

Eth1/23/3,

Eth1/24/2,

Eth1/25/1,

Eth1/25/2, Eth1/25/3

Eth1/26/1, Eth1/26/2

Eth1/26/4, Eth1/27/1

Eth1/27/3, Eth1/27/4

Eth1/28/2, Eth1/28/3

Eth1/29/1, Eth1/29/2

Eth1/29/4, Eth1/30/1

Eth1/30/3, Eth1/30/4

Eth1/31/2, Eth1/31/3

Eth1/32/1, Eth1/32/2

Eth1/32/4, Eth1/33/1

Eth1/33/3, Eth1/33/4

Eth1/34/2, Eth1/34/3

Eth1/35/1, Eth1/35/2

Eth1/35/4, Eth1/36/1

Eth1/36/3, Eth1/36/4

Eth1/37/2, Eth1/37/3

Eth1/38/1, Eth1/38/2

Eth1/38/4, Eth1/39/1

Eth1/39/3, Eth1/39/4

Eth1/40/2, Eth1/40/3

Eth1/41/1, Eth1/41/2

Eth1/41/4, Eth1/42/1

Eth1/25/4,

Eth1/26/3,

Eth1/27/2,

Eth1/28/1,

Eth1/28/4,

Eth1/29/3,

Eth1/30/2,

Eth1/31/1,

Eth1/31/4,

Eth1/32/3,

Eth1/33/2,

Eth1/34/1,

Eth1/34/4,

Eth1/35/3,

Eth1/36/2,

Eth1/37/1,

Eth1/37/4,

Eth1/38/3,

Eth1/39/2,

Eth1/40/1,

Eth1/40/4,

Eth1/41/3,

Eth1/42/2,

Eth1/42/3, Eth1/42/4

Eth1/43/2, Eth1/43/3

Eth1/44/1, Eth1/44/2

Eth1/44/4, Eth1/45/1

Eth1/45/3, Eth1/45/4

Eth1/46/2, Eth1/46/3

Eth1/47/1, Eth1/47/2

Eth1/47/4, Eth1/48/1

Eth1/48/3, Eth1/48/4

Eth1/49/2, Eth1/49/3

Eth1/50/1, Eth1/50/2

Eth1/50/4, Eth1/51/1

Eth1/51/3, Eth1/51/4

Eth1/52/2, Eth1/52/3

Eth1/53/1, Eth1/53/2

Eth1/53/4, Eth1/54/1

Eth1/54/3, Eth1/54/4

Eth1/55/2, Eth1/55/3

Eth1/56/1, Eth1/56/2

Eth1/56/4, Eth1/57/1

Eth1/57/3, Eth1/57/4

Eth1/58/2, Eth1/58/3

Eth1/59/1, Eth1/59/2

Eth1/43/1,

Eth1/43/4,

Eth1/44/3,

Eth1/45/2,

Eth1/46/1,

Eth1/46/4,

Eth1/47/3,

Eth1/48/2,

Eth1/49/1,

Eth1/49/4,

Eth1/50/3,

Eth1/51/2,

Eth1/52/1,

Eth1/52/4,

Eth1/53/3,

Eth1/54/2,

Eth1/55/1,

Eth1/55/4,

Eth1/56/3,

Eth1/57/2,

Eth1/58/1,

Eth1/58/4,

Eth1/59/3,

Eth1/59/4, Eth1/60/1

Eth1/60/2,

Eth1/60/3, Eth1/60/4

Eth1/61/1,

Eth1/61/2, Eth1/61/3

Eth1/61/4,

Eth1/62/1, Eth1/62/2

Eth1/62/3, Eth1/62/4

cs1# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1/1	1	trunking	--
Eth1/1/2	1	trunking	--
Eth1/1/3	1	trunking	--
Eth1/1/4	1	trunking	--
Eth1/2/1	1	trunking	--
Eth1/2/2	1	trunking	--
Eth1/2/3	1	trunking	--
Eth1/2/4	1	trunking	--
.			
.			
.			
Eth1/62/2	none		
Eth1/62/3	none		
Eth1/62/4	none		
Eth1/63	none		
Eth1/64	none		
Pol	1		



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

4. 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       Eth1/63 (P)      Eth1/64 (P)
999    Po999 (SD)    Eth       NONE       --
```

```
cs1#
```

5. 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					
01	e7a	node1-01_clus1	up/up	169.254.36.44/16	node1-
		true			
		node1-01_clus2	up/up	169.254.7.5/16	node1-
01	e7b	true			
		node1-02_clus1	up/up	169.254.197.206/16	node1-
02	e7a	true			
		node1-02_clus2	up/up	169.254.195.186/16	node1-
02	e7b	true			
		node1-03_clus1	up/up	169.254.192.49/16	node1-
03	e7a	true			
		node1-03_clus2	up/up	169.254.182.76/16	node1-
03	e7b	true			
		node1-04_clus1	up/up	169.254.59.49/16	node1-
04	e7a	true			
		node1-04_clus2	up/up	169.254.62.244/16	node1-
04	e7b	true			

8 entries were displayed.

Si alguna LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

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

6. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

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

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

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

Muestra el ejemplo

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

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		

node1-01		
6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-02_clus1
none		
6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-02_clus1
none		
node1-02		
6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-01_clus1
none		
6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-01_clus2
none		
.		
.		
.		

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

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node1-04
Getting addresses from network interface table...
Cluster node1-01_clus1 169.254.36.44 node1-01 e7a
Cluster node1-01_clus2 169.254.7.5 node1-01 e7b
Cluster node1-02_clus1 169.254.197.206 node1-02 e7a
Cluster node1-02_clus2 169.254.195.186 node1-02 e7b
Cluster node1-03_clus1 169.254.192.49 node1-03 e7a
Cluster node1-03_clus2 169.254.182.76 node1-03 e7b
Cluster node1-04_clus1 169.254.59.49 node1-04 e7a
Cluster node1-04_clus2 169.254.62.244 node1-04 e7b
Local = 169.254.59.49 169.254.62.244
Remote = 169.254.36.44 169.254.7.5 169.254.197.206 169.254.195.186
169.254.192.49 169.254.182.76
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 169.254.59.49 to Remote 169.254.182.76
    Local 169.254.59.49 to Remote 169.254.192.49
    Local 169.254.59.49 to Remote 169.254.195.186
    Local 169.254.59.49 to Remote 169.254.197.206
    Local 169.254.59.49 to Remote 169.254.36.44
    Local 169.254.59.49 to Remote 169.254.7.5
    Local 169.254.62.244 to Remote 169.254.182.76
    Local 169.254.62.244 to Remote 169.254.192.49
    Local 169.254.62.244 to Remote 169.254.195.186
    Local 169.254.62.244 to Remote 169.254.197.206
    Local 169.254.62.244 to Remote 169.254.36.44
    Local 169.254.62.244 to Remote 169.254.7.5
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

El futuro

Después de haber actualizado su RCF, ["verificar la configuración de SSH"](#) .

Compruebe su configuración SSH

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

Pasos

1. Compruebe que SSH está habilitado:

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

2. Compruebe que las claves SSH estén habilitadas:

```
show ssh key
```

Muestra el ejemplo

```
(switch)# show ssh key
```

```
rsa Keys generated:Thu May 15 15:09:55 2025
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQgQDCQJPZk7OGhg0j1t0NWKylnI8R8zDpuMpU6KKA  
jPOCShTFpibeYQqxOPTCAKACkut8dduZmc3bY9DIOle0cKYQ8PgS2mG9ovQ0RJ56RUNh  
VNPdJuhXM4ckHoiVJxIAbHkbcw8rzawbkT6cNBUiZY3MrOMh0e0CnMRhh9we  
MOo/vQ==
```

```
bitcount:1024
```

```
fingerprint:
```

```
SHA256:TMUXFgyRC3EcIZEVbQ/P0elDByBCJizPJlXKMkIXfPI
```

```
could not retrieve dsa key information
```

```
ecdsa Keys generated:Thu May 15 15:12:09 2025
```

```
ecdsa-sha2-nistp521
```

```
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBADquZcNSDA/eLAa  
ItXyxVZxsSJSSE3u4et9B6+RLq162zTe/3A6JTCyBrkfrMhQt9QMQ7XrMqJGxLSinXhyU  
ClBxwQD/ZbkZueZHiFuYg5hKN97wUYvts+EwpG2mSVonxKKp  
atmtgu48BqKfZTc4LZYL5vgdh5uuktJ0Z8mYHt3xKPXsvw==
```

```
bitcount:521
```

```
fingerprint:
```

```
SHA256:K8LDx6L7sJjLFn8iubUhjt66uk8TYmXwnQKWVD04C1o
```

```
**
```

```
(switch)# show feature | include scpServer
```

```
scpServer 1 enabled
```

```
(switch)# show feature | include ssh
```

```
sshServer 1 enabled
```

```
(switch)#
```

El futuro

Después de haber verificado su configuración SSH, ["configurar la monitorización del estado del conmutador"](#).

Restablecer el interruptor 9364D-GX2A a los valores predeterminados de fábrica

Para restablecer el interruptor 9364D-GX2A a los valores predeterminados de fábrica, debe borrar la configuración del interruptor 9364D-GX2A.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Borrar la configuración existente:

```
write erase
```

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

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

2. Recargue el software del conmutador:

```
reload
```

```
(cs2)# reload
```

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

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

Reemplazar un conmutador Cisco Nexus 9364D-GX2A

Siga estos pasos para reemplazar un conmutador Nexus 9364D-GX2A defectuoso en una red de clúster. Este es un procedimiento no disruptivo (NDU).

Revise los requisitos

Antes de realizar la sustitución del interruptor, asegúrese de que:

- Ha verificado el número de serie del interruptor para asegurarse de que se sustituye el interruptor correcto.
- 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 ONTAP `cluster ping-cluster -node <node-name>` El comando debe indicar que la conectividad básica y la comunicación mayor que PMTU son exitosas en todas las rutas.
- En el interruptor de reemplazo Nexus 9364D-GX2A:
 - 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 1/62.
 - Todos los puertos de enlace entre conmutadores (ISL) están deshabilitados en los puertos 1/63 y 1/64.
 - El archivo de configuración de referencia (RCF) y el conmutador de imagen del sistema operativo NX-OS se cargan en el conmutador.
 - La personalización inicial del conmutador está completa, como se detalla en ["Configurar el conmutador de clúster 9364D-GX2A"](#).

Cualquier personalización de sitio anterior, como STP, SNMP y SSH, se copian al nuevo switch.

- Ha ejecutado el comando para migrar una LIF de clúster desde el nodo en el que se aloja la LIF del clúster.

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después de las tareas de mantenimiento para deshabilitar la creación de casos durante el mantenimiento. Consulte este artículo de la base de conocimientos ["SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#) para obtener más detalles.
- Habilite el registro de sesiones para cualquier sesión de CLI. Para obtener instrucciones sobre cómo activar el registro de sesiones, consulte la sección «Salida de sesión de registro» de este artículo de la base de conocimientos ["Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP"](#).

Sustituya el interruptor

Acerca de los ejemplos

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

- Los nombres de los conmutadores Nexus 9364D-GX2A existentes son cs1 y cs2.
- El nombre del nuevo conmutador Nexus 9364D-GX2A es newcs2.
- Los nombres de los nodos son node1-01, node1-02, node1-03 y node1-04.
- Los nombres de clúster LIF son node1-01_clus1 y node1-01_clus2 para el nodo1-01, node1-02_clus1 y node1-02_clus2 para el nodo1-02, node1-03_clus1 y node1-03_clus2 para el nodo1-03, y node1-04_clus1 y node1-04_clus2 para el nodo1-04.
- El símbolo del sistema de cambios en todos los nodos del cluster es cluster1:*>

Acerca de esta tarea

El siguiente procedimiento se basa en la siguiente topología de red de clúster:

Muestra el ejemplo

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

Node: node1-01

Ignore

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

e7a	Cluster	Cluster		up	9000	auto/10000	healthy
false							
e7b	Cluster	Cluster		up	9000	auto/10000	healthy
false							

Node: node1-02

Ignore

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

e7a	Cluster	Cluster		up	9000	auto/10000	healthy
false							
e7b	Cluster	Cluster		up	9000	auto/10000	healthy
false							

Node: node1-03

Ignore

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

e7a	Cluster	Cluster		up	9000	auto/10000	healthy
false							
e7b	Cluster	Cluster		up	9000	auto/10000	healthy
false							

Node: node1-04

Ignore

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

e7a	Cluster	Cluster		up	9000	auto/10000
false						healthy
e7b	Cluster	Cluster		up	9000	auto/10000
false						healthy

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

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

Cluster				
	node1-01_clus1	up/up	169.254.209.69/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.49.125/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.47.194/16	node1-02
e7a	true			
	node1-02_clus2	up/up	169.254.19.183/16	node1-02
e7b	true			
.				
.				
.				

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

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

node1-01/cdp				
	e10a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/3	N9K-
C9364D-GX2A				
	e10b	cs2 (FDOXXXXXXXXX)	Ethernet1/16/3	N9K-
C9364D-GX2A				
	e11a	cs1 (FLMXXXXXXXXX)	Ethernet1/16/4	N9K-

```

C9364D-GX2A
    e11b    cs2 (FDOXXXXXXXXX)      Ethernet1/16/4    N9K-
C9364D-GX2A
    e1a     cs1 (FLMXXXXXXXXX)      Ethernet1/16/1    N9K-
C9364D-GX2A
    e1b     cs2 (FDOXXXXXXXXX)      Ethernet1/16/1    N9K-
C9364D-GX2A
    .
    .
    .
    e7a     cs1 (FLMXXXXXXXXX)      Ethernet1/16/2    N9K-
C9364D-GX2A
    e7b     cs2 (FDOXXXXXXXXX)      Ethernet1/16/2    N9K-
C9364D-GX2A
    .
    .
    .

```

```
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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform	
newcs2 (FDOXXXXXXXXX) Eth1/31	Eth1/63	179	R S I s	N9K-C9332D-GX2B	
newcs2 (FDOXXXXXXXXX) Eth1/32	Eth1/64	179	R S I s	N9K-C9332D-GX2B	
node1-01 e1a	Eth1/4/1	123	H	AFX-1K	
node1-01 e7a	Eth1/4/2	123	H	AFX-1K	
node1-01 e10a	Eth1/4/3	123	H	AFX-1K	
node1-01 e11a	Eth1/4/4	123	H	AFX-1K	
node1-02 e1a	Eth1/9/1	138	H	AFX-1K	
node1-02 e7a	Eth1/9/2	138	H	AFX-1K	
node1-02	Eth1/9/3	138	H	AFX-1K	


```

e10a
node1-02          Eth1/9/4          138    H          AFX-1K
e11a
node1-03          Eth1/15/1         138    H          AFX-1K
e1a
node1-03          Eth1/15/2         138    H          AFX-1K
e7a
node1-03          Eth1/15/3         138    H          AFX-1K
e10a
node1-03          Eth1/15/4         138    H          AFX-1K
e11a
node1-04          Eth1/16/1         173    H          AFX-1K
e1a
node1-04          Eth1/16/2         173    H          AFX-1K
e7a
node1-04          Eth1/16/3         173    H          AFX-1K
e10a
node1-04          Eth1/16/4         173    H          AFX-1K
e11a

```

Total entries displayed: 18

newcs2# **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
cs1(FDOXXXXXXXXX) Eth1/31	Eth1/63	179	R S I s	N9K-C9332D-GX2B
cs1(FDOXXXXXXXXX) Eth1/32	Eth1/64	179	R S I s	N9K-C9332D-GX2B
node1-01 e1a	Eth1/4/1	123	H	AFX-1K
node1-01 e7a	Eth1/4/2	123	H	AFX-1K
node1-01 e10a	Eth1/4/3	123	H	AFX-1K
node1-01 e11a	Eth1/4/4	123	H	AFX-1K
node1-02 e1a	Eth1/9/1	138	H	AFX-1K

node1-02 e7a	Eth1/9/2	138	H	AFX-1K
node1-02 e10a	Eth1/9/3	138	H	AFX-1K
node1-02 e11a	Eth1/9/4	138	H	AFX-1K
node1-03 e1a	Eth1/15/1	138	H	AFX-1K
node1-03 e7a	Eth1/15/2	138	H	AFX-1K
node1-03 e10a	Eth1/15/3	138	H	AFX-1K
node1-03 e11a	Eth1/15/4	138	H	AFX-1K
node1-04 e1a	Eth1/16/1	173	H	AFX-1K
node1-04 e7a	Eth1/16/2	173	H	AFX-1K
node1-04 e10a	Eth1/16/3	173	H	AFX-1K
node1-04 e11a	Eth1/16/4	173	H	AFX-1K

Total entries displayed: 18

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
```

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. 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 Descarga.
 - 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.
3. 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
newcs2(config)# interface e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7/1-4,e1/8/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/9/1-4,e1/10/1-4,e1/11/1-4,e1/12/1-4,e1/13/1-4,e1/14/1-4,e1/15/1-4,e1/16/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/17/1-4,e1/18/1-4,e1/19/1-4,e1/20/1-4,e1/21/1-4,e1/22/1-4,e1/23/1-4,e1/24/1-4
csnewcs21(config-if-range)# shutdown
newcs2(config)# interface e1/25/1-4,e1/26/1-4,e1/27/1-4,e1/28/1-4,e1/29/1-4,e1/30/1-4,e1/31/1-4,e1/32/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/33/1-4,e1/34/1-4,e1/35/1-4,e1/36/1-4,e1/37/1-4,e1/38/1-4,e1/39/1-4,e1/40/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/41/1-4,e1/42/1-4,e1/43/1-4,e1/44/1-4,e1/35/1-4,e1/46/1-4,e1/47/1-4,e1/48/1-4
newcs2(config-if-range)# shutdown
newcs2(config)# interface e1/49/1-4,e1/50/1-4,e1/51/1-4,e1/52/1-4,e1/53/1-4,e1/54/1-4,e1/55/1-4,e1/56/1-4
newcs2(config-if-range)# shutdown\
newcs2(config)# interface e1/57/1-4,e1/58/1-4,e1/59/1-4,e1/60/1-4,e1/61/1-4,e1/62/1-4
newcs2(config-if-range)# shutdown
newcs2(config-if-range)# exit
newcs2(config)# exit
```

4. 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	node1-01_clus1	true
Cluster	node1-01_clus2	true
Cluster	node1-02_clus1	true
Cluster	node1-02_clus2	true
Cluster	node1-03_clus1	true
Cluster	node1-03_clus2	true
Cluster	node1-04_clus1	true
Cluster	node1-04_clus2	true

8 entries were displayed.

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

- Puedes utilizar el `network interface check cluster-connectivity show` Comando para mostrar los detalles de una verificación de accesibilidad para la conectividad del clúster:

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

Muestra el ejemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-
02_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-
02_clus2	none		
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-
01_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-
01_clus2	none		
.			
.			
.			

- b. Alternativamente, también puedes utilizar el `cluster ping-cluster -node <node-name>` Comando para comprobar la conectividad:

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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 1/63 y 1/64 en el conmutador Nexus 9364D-GX2A cs1.

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/63-64
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit
```

2. Retire todos los cables del conmutador cs2 Nexus 9364D-GX2B y luego conéctelos a los mismos puertos en el conmutador newcs2 Nexus 9364D-GX2A.
3. Active los puertos ISL 1/63 y 1/64 entre los conmutadores cs1 y newcs2 y luego verifique el estado de funcionamiento del canal del puerto.

El canal del puerto debe indicar Po1(SU) y los puertos miembros deben indicar Eth1/63(P) y Eth1/64(P).

Muestra el ejemplo

Este ejemplo habilita los puertos ISL 1/63 y 1/64 y muestra el resumen del canal del puerto en el conmutador cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/63-64
cs1(config-if-range)# no shutdown
cs1(config-if-range)# exit
cs1(config)# exit
cs1#
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
-----
-----
11      Po1 (SU)      Eth      LACP      Eth1/63 (P)  Eth1/64 (P)
999     Po999 (SD)    Eth      NONE      --
```

4. Verifique que el puerto e7b 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: node1-01

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-02

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-03

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	


```

healthy false
e7b          Cluster      Cluster      up    9000  auto/100000
healthy false

Node: node1-04

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e7a        Cluster      Cluster      up    9000  auto/100000
healthy false
e7b        Cluster      Cluster      up    9000  auto/100000
healthy false

8 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, el nodo LIF node1-01_clus2 en el nodo1-01 se revierte exitosamente si el valor de Inicio es verdadero y el puerto es e7b.

Los siguientes comandos devuelven LIF node1-01_clus2 en node1-01 al puerto base e7a y muestra información sobre los LIF en ambos nodos. La activación del primer nodo se realiza correctamente si la columna Is Home es verdadera para ambas interfaces del clúster y muestran las asignaciones de puerto correctas, en este ejemplo e7a y e7b en el nodo1-01.

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

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

Cluster				
	node1-01_clus1	up/up	169.254.209.69/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.49.125/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.47.194/16	node1-02
e7b	true			
	node1-02_clus2	up/up	169.254.19.183/16	node1-02
e7a	false			
	.			
	.			
	.			

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
-----	-----	-----
node1-01	false	true
node1-02	true	true
node1-03	true	true
node1-04	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: node1-01

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node1-02

Ignore

						Speed(Mbps)	Health
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----		
-----	-----						
e7a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e7b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

.
. .
. .

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

- Puedes utilizar el `network interface check cluster-connectivity show` Comando para mostrar los detalles de una verificación de accesibilidad para la conectividad del clúster:

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

Muestra el ejemplo

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1-01			
	6/4/2025 03:13:33 -04:00	node1-01_clus2	node1-
02_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-01_clus2	node1-
02_clus2	none		
node1-02			
	6/4/2025 03:13:33 -04:00	node1-02_clus2	node1-
01_clus1	none		
	6/4/2025 03:13:34 -04:00	node1-02_clus2	node1-
01_clus2	none		
.			
.			
.			

- b. Alternativamente, también puedes utilizar el `cluster ping-cluster -node <node-name>` Comando para comprobar la conectividad:

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

Muestra el ejemplo

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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 3: Verificar la configuración

1. Verificar el estado de todos los puertos del clúster.

a. Puertos de clúster

- i. Compruebe que los puertos del clúster estén en buen estado en todos los nodos del clúster:

```
network port show ipspace Cluster
```

```
network interface show -vserver cluster
```

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

```
show cdp neighbors
```

Muestra el ejemplo

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

```
Node: node1-01
```

```
Ignore
```

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	----	-----
-----	-----				
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

```
Node: node1-02
```

```
Ignore
```

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	----	-----
-----	-----				
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

```
Node: node1-03
```

```
Ignore
```

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	----	-----
-----	-----				
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node1-04

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e7a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e7b	Cluster	Cluster		up	9000
healthy	false				auto/100000

cluster1::*> **network interface show -vserver cluster**

	Logical	Status	Network	
Current	Current	Is		
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
Cluster				
01	node1-01_clus1	up/up	169.254.209.69/16	node1-
	e7a	true		
01	node1-01_clus2	up/up	169.254.49.125/16	node1-
	e7b	true		
02	node1-02_clus1	up/up	169.254.47.194/16	node1-
	e7b	true		
02	node1-02_clus2	up/up	169.254.19.183/16	node1-
	e7a	false		
	.			
	.			
	.			

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

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			
-----	-----	-----	-----
node1-01/cdp			

```

          e10a    cs1 (FLMXXXXXXXXX)      Ethernet1/16/3
N9K-C9364D-GX2A
          e10b    cs2 (FDOXXXXXXXXX)      Ethernet1/16/3
N9K-C9364D-GX2A
          e11a    cs1 (FLMXXXXXXXXX)      Ethernet1/16/4
N9K-C9364D-GX2A
          e11b    cs2 (FDOXXXXXXXXX)      Ethernet1/16/4
N9K-C9364D-GX2A
          e1a     cs1 (FLMXXXXXXXXX)      Ethernet1/16/1
N9K-C9364D-GX2A
          e1b     cs2 (FDOXXXXXXXXX)      Ethernet1/16/1
N9K-C9364D-GX2A
          .
          .
          .
          e7a     cs1 (FLMXXXXXXXXX)      Ethernet1/16/2
N9K-C9364D-GX2A
          e7b     cs2 (FDOXXXXXXXXX)      Ethernet1/16/2
N9K-C9364D-GX2A
          .
          .
          .

```

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			
newcs2 (FDOXXXXXXXXX)	Eth1/63	179	R S I s	N9K-
C9332D-GX2B	Eth1/31			
newcs2 (FDOXXXXXXXXX)	Eth1/64	179	R S I s	N9K-
C9332D-GX2B	Eth1/32			
node1-01	Eth1/4/1	123	H	AFX-1K
e1a				
node1-01	Eth1/4/2	123	H	AFX-1K
e7a				
node1-01	Eth1/4/3	123	H	AFX-1K
e10a				
node1-01	Eth1/4/4	123	H	AFX-1K
e11a				

node1-02	Eth1/9/1	138	H	AFX-1K
e1a				
node1-02	Eth1/9/2	138	H	AFX-1K
e7a				
node1-02	Eth1/9/3	138	H	AFX-1K
e10a				
node1-02	Eth1/9/4	138	H	AFX-1K
e11a				
node1-03	Eth1/15/1	138	H	AFX-1K
e1a				
node1-03	Eth1/15/2	138	H	AFX-1K
e7a				
node1-03	Eth1/15/3	138	H	AFX-1K
e10a				
node1-03	Eth1/15/4	138	H	AFX-1K
e11a				
node1-04	Eth1/16/1	173	H	AFX-1K
e1a				
node1-04	Eth1/16/2	173	H	AFX-1K
e7a				
node1-04	Eth1/16/3	173	H	AFX-1K
e10a				
node1-04	Eth1/16/4	173	H	AFX-1K
e11a				

Total entries displayed: 18

newcs2# **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 (FDOXXXXXXXXX)	Eth1/63	179	R S I s	N9K-
C9332D-GX2B	Eth1/31			
cs1 (FDOXXXXXXXXX)	Eth1/64	179	R S I s	N9K-
C9332D-GX2B	Eth1/32			
node1-01	Eth1/4/1	123	H	AFX-1K
e1a				
node1-01	Eth1/4/2	123	H	AFX-1K

```

e7a
node1-01          Eth1/4/3          123      H          AFX-1K
e10a
node1-01          Eth1/4/4          123      H          AFX-1K
e11a
node1-02          Eth1/9/1          138      H          AFX-1K
e1a
node1-02          Eth1/9/2          138      H          AFX-1K
e7a
node1-02          Eth1/9/3          138      H          AFX-1K
e10a
node1-02          Eth1/9/4          138      H          AFX-1K
e11a
node1-03          Eth1/15/1         138      H          AFX-1K
e1a
node1-03          Eth1/15/2         138      H          AFX-1K
e7a
node1-03          Eth1/15/3         138      H          AFX-1K
e10a
node1-03          Eth1/15/4         138      H          AFX-1K
e11a
node1-04          Eth1/16/1         173      H          AFX-1K
e1a
node1-04          Eth1/16/2         173      H          AFX-1K
e7a
node1-04          Eth1/16/3         173      H          AFX-1K
e10a
node1-04          Eth1/16/4         173      H          AFX-1K
e11a

```

Total entries displayed: 18

b. Puertos HA

- i. Verifique que todos los puertos HA estén activos con un estado saludable:

```
ha interconnect status show -node <node-name>
```

Muestra el ejemplo

```
cluster1::*> ha interconnect status show -node node1-01
(system ha interconnect status show)
```

```

        Node: node1-01
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
        Port Name: elb-18
        MTU: 4096
        Link Information: ACTIVE
```

```
cluster1::*> ha interconnect status show -node node1-02
(system ha interconnect status show)
```

```

        Node: node1-02
        Link 0 Status: up
        Link 1 Status: up
        Is Link 0 Active: true
        Is Link 1 Active: true
        IC RDMA Connection: up
        Slot: 0
        Debug Firmware: no
```

```
Interconnect Port 0 :
        Port Name: ela-17
        MTU: 4096
        Link Information: ACTIVE
```

```
Interconnect Port 1 :
```

```
Port Name: e1b-18
MTU: 4096
Link Information: ACTIVE
```

```
.
.
.
```

a. Puertos de almacenamiento

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

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

Muestra el ejemplo

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

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

node1-01	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-02	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
node1-03	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
node1-04	e10a	ENET	-	100	enabled	online
	e10b	ENET	-	100	enabled	online
	e11a	ENET	-	100	enabled	online
	e11b	ENET	-	100	enabled	online
16 entries were displayed.						

b. Puertos para estantes de almacenamiento

- i. Verifique que todos los puertos del estante de almacenamiento estén activos con un estado saludable:

```
storage shelf port show
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show
```

Shelf	ID	Module	State	Internal?
-----	--	-----	-----	-----
1.1				
	0	A	connected	false
	1	A	connected	false
	2	A	connected	false
	3	A	connected	false
	4	A	connected	false
	5	A	connected	false
	6	A	connected	false
	7	A	connected	false
	8	B	connected	false
	9	B	connected	false
	10	B	connected	false
	11	B	connected	false
	12	B	connected	false
	13	B	connected	false
	14	B	connected	false
	15	B	connected	false

```
16 entries were displayed.
```

- ii. Verifique el estado de conexión de todos los puertos del estante de almacenamiento:

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

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-  
device,remote-port,connector-state
```

shelf	id	connector-state	remote-port	remote-device
1.1	0	connected	Ethernet1/17/1	CX9332D-cs1
1.1	1	connected	Ethernet1/15/1	CX9364D-cs1
1.1	2	connected	Ethernet1/17/2	CX9332D-cs1
1.1	3	connected	Ethernet1/15/2	CX9364D-cs1
1.1	4	connected	Ethernet1/17/3	CX9332D-cs1
1.1	5	connected	Ethernet1/15/3	CX9364D-cs1
1.1	6	connected	Ethernet1/17/4	CX9332D-cs1
1.1	7	connected	Ethernet1/15/4	CX9364D-cs1
1.1	8	connected	Ethernet1/19/1	CX9332D-cs1
1.1	9	connected	Ethernet1/17/1	CX9364D-cs1
1.1	10	connected	Ethernet1/19/2	CX9332D-cs1
1.1	11	connected	Ethernet1/17/2	CX9364D-cs1
1.1	12	connected	Ethernet1/19/3	CX9332D-cs1
1.1	13	connected	Ethernet1/17/3	CX9364D-cs1
1.1	14	connected	Ethernet1/19/4	CX9332D-cs1
1.1	15	connected	Ethernet1/17/4	CX9364D-cs1

```
16 entries were displayed.
```

2. 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
```

El futuro

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

Switches de clúster

BES-53248 compatible con Broadcom

Manos a la obra

Flujo de trabajo de instalación y configuración de los conmutadores BES-53248

BES-53248 es un switch nativo diseñado para funcionar en clústeres de ONTAP que van desde dos hasta 24 nodos.

Siga estos pasos de flujo de trabajo para instalar y configurar sus conmutadores BES-53248.

1

"Revisar los requisitos de configuración"

Revise los requisitos de configuración para el conmutador de clúster BES-53248.

2

"Revise los componentes y números de pieza"

Revise los componentes y números de pieza del conmutador de grupo BES-53248.

3

"Revisar la documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores BES-53248 y el clúster ONTAP .

4

"Instale el hardware"

Instale el hardware del interruptor.

5

"Configurar el software"

Configurar el software del conmutador.

Requisitos de configuración para los switches de clúster BES-53248

Para la instalación y el mantenimiento del conmutador BES-53248, asegúrese de revisar los requisitos de soporte y configuración de EFOS y ONTAP.

Soporte para EFOS y ONTAP

Consulte ["Hardware Universe de NetApp"](#) y.. ["Matriz de compatibilidad de switches Broadcom"](#) Para obtener información sobre compatibilidad de EFOS y ONTAP con conmutadores BES-53248. La compatibilidad con EFOS y ONTAP puede variar según el tipo de máquina específico del interruptor BES-53248. Para obtener información detallada sobre todos los tipos de máquinas de conmutación BES-52348, consulte ["Componentes y números de pieza para switches de clúster BES-53248"](#).

Requisitos de configuración

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

Asignaciones de puertos del switch del clúster

Puede utilizar la tabla de asignaciones de puertos de conmutador de clúster BES-53248 compatible con Broadcom como guía para configurar su clúster.

Puertos del switch	Uso de puertos
01-16	Configuración base de nodos de puertos de clúster de 10 GbE
17-48	Nodos de puertos de clúster de 10 GbE, con licencias
49-54	40/100GbE nodos de puertos en clúster, con licencias, añadidos a la derecha a la izquierda
55-56	Puertos de enlace entre switches (ISL) de clúster de 100 GbE, configuración base

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

Limitación de velocidad del grupo de puertos

- En los switches de clúster BES-53248, los puertos de 48 10 GbE (SFP28/SFP+) se combinan en 12 grupos de puertos de 4 de la siguiente manera: Puertos 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44, y 45-48.
- La velocidad del puerto SFP28/SFP+ debe ser la misma (10 GbE o 25 GbE) en todos los puertos del grupo de 4 puertos.

Requisitos adicionales

- Si compra licencias adicionales, consulte "[Activar puertos de licencias nuevas](#)" para obtener detalles sobre cómo activarlos.
- Si SSH está activo, debe volver a habilitarlo manualmente después de ejecutar el comando `erase startup-config` y reiniciando el interruptor.

¿Qué sigue?

["Componentes y números de pieza"](#) .

Componentes y números de pieza para switches de clúster BES-53248

Para la instalación y mantenimiento del conmutador BES-53248, asegúrese de revisar la lista de componentes y números de pieza.

En la siguiente tabla se enumeran el número de pieza, la descripción y las versiones mínimas de EFOS y ONTAP para los componentes del conmutador de clúster BES-53248, incluidos los detalles del kit de guías de montaje en bastidor.



Se requiere una versión EFOS mínima de **3.10.0.3** para los números de pieza **X190005-B** y **X190005R-B**.

Número de pieza	Descripción	Versión mínima de EFOS	Versión de ONTAP mínima
X190005-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PTSX (PTSX = escape del lado del puerto)	3.10.0.3	9.8
X190005R-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PSIN (PSIN = entrada lateral del puerto)	3.10.0.3	9.8
X190005	BES-53248, CLSW, 16PT10/25GB, PTSX, SOPORTE BRDCM	3.4.4.6	9.5P8
X190005R	BES-53248, CLSW, 16PT10/25GB, PSIN, BRDCM SUPP	3.4.4.6	9.5P8
X-RAIL-4POST-190005	Kit de rieles para montaje en rack Ozeki 4 post 19"	N.A.	N.A.



Tenga en cuenta la siguiente información con respecto a los tipos de máquinas:

Tipo de máquina	Versión mínima de EFOS
BES-53248A1	3.4.4.6
BES-53248A2	3.10.0.3
BES-53248A3	3.10.0.3

Puede determinar su tipo de máquina específico mediante el comando: `show version`

Muestra el ejemplo

```
(cs1)# show version
```

```
Switch: cs1
```

```
System Description..... EFOS, 3.10.0.3, Linux  
5.4.2-b4581018, 2016.05.00.07
```

```
Machine Type..... BES-53248A3
```

```
Machine Model..... BES-53248
```

```
Serial Number..... QTCU225xxxxx
```

```
Part Number..... 1IX8BZxxxxx
```

```
Maintenance Level..... a3a
```

```
Manufacturer..... QTMC
```

```
Burned In MAC Address..... C0:18:50:F4:3x:xx
```

```
Software Version..... 3.10.0.3
```

```
Operating System..... Linux 5.4.2-b4581018
```

```
Network Processing Device..... BCM56873_A0
```

```
.  
.   
.
```

¿Qué sigue?

["Documentación requerida"](#) .

Requisitos de documentación para los switches de clúster BES-53248

Para la instalación y mantenimiento del conmutador BES-53248, asegúrese de revisar la documentación específica del conmutador y del controlador.

Documentación de Broadcom

Para configurar el switch de clúster BES-53248, necesita los siguientes documentos disponibles en el sitio de soporte de Broadcom: ["Línea de producto de conmutador Ethernet Broadcom"](#)

Título del documento	Descripción
<i>EFOS Guía del administrador v3.4.3</i>	Proporciona ejemplos de cómo utilizar el conmutador BES-53248 en una red típica.
<i>Referencia de comandos de la CLI del EFOS v3.4.3</i>	Describe los comandos de la interfaz de línea de comandos (CLI) que utiliza para ver y configurar el software BES-53248.
<i>Guía de puesta en marcha del EFOS v3.4.3</i>	Proporciona información detallada acerca del conmutador BES-53248.

Título del documento	Descripción
<i>EFOS SNMP Reference Guide v3.4.3</i>	Proporciona ejemplos de cómo utilizar el conmutador BES-53248 en una red típica.
<i>EFOS escala parámetros y valores v3.4.3</i>	Describe los parámetros de escala predeterminados con los que se suministra y valida el software EFOS en las plataformas compatibles.
<i>EFOS Especificaciones funcionales v3.4.3</i>	Describe las especificaciones del software EFOS en las plataformas compatibles.
<i>Notas de publicación de EFOS v3.4.3</i>	Proporciona información específica de la versión sobre el software BES-53248.
<i>Matriz de compatibilidad de redes de administración y redes de clúster</i>	Proporciona información sobre la compatibilidad de red. La matriz está disponible en el sitio de descarga del conmutador BES-53248 en "Switches de clúster Broadcom" .

Documentación de los sistemas ONTAP y artículos de la base de conocimientos

Para configurar un sistema ONTAP, necesita los siguientes documentos en el sitio de soporte de NetApp en ["mysupport.netapp.com"](http://mysupport.netapp.com) O el sitio de la base de conocimientos (KB) en ["kb.netapp.com"](http://kb.netapp.com).

Nombre	Descripción
"Hardware Universe de NetApp"	Describe los requisitos de alimentación y del sitio para todo el hardware de NetApp, incluidos los armarios de sistema, y proporciona información sobre los conectores y las opciones de cables relevantes que se deben usar junto con sus números de pieza.
<i>Específicos del controlador instrucciones de instalación y configuración</i>	Describe cómo instalar el hardware de NetApp.
ONTAP 9	Proporciona información detallada sobre todos los aspectos de la versión 9 de ONTAP.
<i>Cómo añadir licencias de puerto adicionales para el conmutador BES-53248 compatible con Broadcom</i>	Proporciona información detallada sobre cómo agregar licencias de puerto. Vaya a la "Artículo de base de conocimientos" .

Instale el hardware

Flujo de trabajo de instalación de hardware para conmutadores BES-53248

Para instalar y configurar el hardware de un conmutador de clúster BES-53248, siga estos pasos:

1

"Instalar el hardware del interruptor"

Instalar y configurar el hardware del conmutador BES-53248.

2

"Revisar el cableado y la configuración"

Revise las consideraciones de cableado y configuración para el conmutador de clúster BES-53248.

Instale el hardware para el conmutador de clúster BES-53248

Para instalar el hardware del BES-53248, consulte la documentación de Broadcom.

Pasos

1. Revise la ["requisitos de configuración"](#).
2. Siga las instrucciones de ["Guía de instalación de switches de clúster compatible con BES-53248 de Broadcom"](#).

El futuro

["Revisar el cableado y la configuración"](#) .

Revise las consideraciones sobre el cableado y la configuración

Antes de configurar el conmutador Broadcom BES-53248, revise las siguientes consideraciones.

Asignaciones de switches de puertos de clúster

Puede utilizar la tabla de asignaciones de puertos de switch de clúster BES-53248 compatible con Broadcom como guía para configurar el clúster.

Puertos del conmutador	Uso de puertos
0-16	Configuración base de nodos de puertos de clúster de 10 GbE
17-48	Nodos de puertos de clúster de 10 GbE, con licencias
49-54	40/100GbE nodos de puertos en clúster, con licencias, añadidos a la derecha a la izquierda
55-56	Puertos de enlace entre switches (ISL) de clúster de 100 GbE, configuración base

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

Limitación de velocidad del grupo de puertos

- En los switches de clúster BES-53248, los puertos de 48 10 GbE (SFP28/SFP+) se combinan en 12 grupos de puertos de 4 de la siguiente manera: Puertos 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32,

33-36, 37-40, 41-44, y 45-48.

- La velocidad del puerto SFP28/SFP+ debe ser la misma (10 GbE o 25 GbE) en todos los puertos del grupo de 4 puertos.
- Si las velocidades de un grupo de 4 puertos son diferentes, los puertos del switch no funcionarán correctamente.

Requisitos de FEC

- Para ver los puertos 25G con cables de cobre, consulte la siguiente tabla para obtener más detalles.

Si el lado del controlador es de `auto`, El lado del interruptor está ajustado a FEC 25G.

FAS2820 FEC			Switch FEC			
write	read		write	read		link status
	requested_fec	negotiated_fec		Configured FEC Mode	Physical FEC Status	
fc	FC-FEC/BASE-R	none	No FEC	FEC Disabled	FEC Disabled	UP
fc	FC-FEC/BASE-R	FC-FEC/BASE-R	FEC 25G	FEC 25G	CL-74	UP
auto	RS-FEC	none	FEC 25G	FEC 25G	CL74	UP
auto	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	FEC 25G	FEC 25G	CL74	UP
rs	RS-FEC	none	FEC 25G	FEC 25G	CL74	UP
rs	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	UP

- Para los puertos 25G con cables de fibra óptica, consulte la siguiente tabla para obtener más información:

FAS2820 FEC			Switch FEC			
write	read		write	read		link status
	requested_fec	negotiated_fec		Configured FEC Mode	Physical FEC Status	
fc	FC-FEC/BASE-R	none	No FEC	FEC Disabled	FEC Disabled	DOWN
fc	FC-FEC/BASE-R	FC-FEC/BASE-R	FEC 25G	FEC 25G	CL-74	UP
auto	RS-FEC	none	FEC 25G	FEC 25G	CL74	DOWN
auto	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	DOWN
none	none	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	FEC 25G	FEC 25G	CL74	DOWN
rs	RS-FEC	none	FEC 25G	FEC 25G	CL74	DOWN
rs	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	DOWN

Implantación de Bootarg

Utilice el siguiente comando para establecer el FEC de puerto 25G en cualquiera de los dos `auto` o `fc`, según sea necesario:

```
systemshell -node <node> -command sudo sysctl
dev.ice.<X>.requested_fec=<auto/fc>
```

- Cuando se establece en **auto**:
 - La `auto` la configuración propaga la configuración al hardware inmediatamente y no es necesario reiniciarla.
 - Si `bootarg.cpk_fec_fc_eXx` already exists, se elimina del almacenamiento de arranque.
 - Después de un reinicio, el `auto` el ajuste permanece en su lugar desde `auto` Es el valor predeterminado de FEC.
- Cuando se establece en **fc**:
 - La `FC-FEC` la configuración propaga la configuración al hardware inmediatamente y no es necesario reiniciarla.
 - Un nuevo `bootarg.cpk_fec_fc_eXx` se crea con el valor establecido en `true`.
 - Después de un reinicio, `FC-FEC` el ajuste permanece en su lugar para que el código de controlador lo utilice.

Configurar el software

Flujo de trabajo de instalación de software para conmutadores BES-53248

Para instalar y configurar el software para un conmutador de clúster BES-53248, siga estos pasos:

1

"Configure el switch"

Configurar el conmutador de clúster BES-53248.

2

"Instale el software del EFOS"

Descargue e instale el software Ethernet Fabric OS (EFOS) en el switch de clúster BES-53248.

3

"Instale licencias para switches de clúster BES-53248"

Opcionalmente, añada nuevos puertos comprando e instalando más licencias. El modelo de base de switches tiene licencia para 16 puertos de 10 GbE o 25 GbE y dos puertos de 100 GbE.

4

"Instalación del archivo de configuración de referencia (RCF)"

Instale o actualice el RCF en el conmutador de clúster BES-53248 y, a continuación, compruebe los puertos para obtener una licencia adicional después de aplicar el RCF.

5

"Habilite SSH en switches de clúster BES-53248"

Si utiliza el monitor de estado del switch Ethernet (CSHM) y las funciones de recopilación de registros, habilite SSH en los switches.

6

"Restablecer el interruptor a los valores predeterminados de fábrica"

Borre la configuración del conmutador de clúster BES-53248.

Configure el conmutador de clúster BES-53248

Siga estos pasos para realizar una configuración inicial del conmutador de clúster BES-53248.

Antes de empezar

- El hardware está instalado, como se describe en ["Instale el hardware"](#).
- Ha revisado lo siguiente:
 - ["Requisitos de configuración"](#)
 - ["Componentes y números de pieza"](#)
 - ["Requisitos de documentación"](#)

Acerca de los ejemplos

Los ejemplos de los procedimientos de configuración utilizan la siguiente nomenclatura de conmutación y

nodo:

- Los nombres de los switches de NetApp son `cs1` y.. `cs2`. La actualización se inicia en el segundo conmutador, `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 de NetApp"](#) para los puertos de clúster reales compatibles con la plataforma.
- Los vínculos entre switches (ISL) compatibles con los switches de NetApp son los puertos 0/55 y 0/56.
- Las conexiones de nodos compatibles con los switches de NetApp son los puertos 0/1 a 0/16, con licencia predeterminada.
- En los ejemplos se utilizan dos nodos, pero puede tener hasta 24 nodos en un clúster.

Pasos

1. Conecte el puerto serie a un host o puerto serie.
2. 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.
3. En la consola, configure los ajustes de serie del lado del host:
 - 115200 baudios
 - 8 bits de datos
 - 1 bit de parada
 - paridad: none
 - control de flujo: ninguno
4. Inicie sesión en el conmutador como `admin` Y pulse **Intro** cuando se le solicite una contraseña. El nombre predeterminado del conmutador es **enrutamiento**. Introduzca, en el aviso del `enable`. Esto le permite acceder al modo EXEC privilegiado para la configuración del switch.

```
User: admin
Password:
(Routing)> enable
Password:
(Routing) #
```

5. Cambie el nombre del conmutador a **cs2**.

```
(Routing) # hostname cs2
(cs2) #
```

6. Para configurar una dirección de administración IPv4 o IPv6 estática para el puerto de servicio del conmutador:

IPv4

el puerto de servicio está configurado para utilizar DHCP de forma predeterminada. La dirección IP, la máscara de subred y la dirección de puerta de enlace predeterminada se asignan automáticamente.

```
(cs2)# serviceport protocol none
(cs2)# network protocol none
(cs2)# serviceport ip <ip-address> <netmask> <gateway>
```

IPv6

el puerto de servicio está configurado para utilizar DHCP de forma predeterminada. La dirección IP, la máscara de subred y la dirección de puerta de enlace predeterminada se asignan automáticamente.

```
(cs2)# serviceport protocol none
(cs2)# network protocol none
(cs2)# serviceport ipv6 <address>
(cs2)# serviceport ipv6 <gateway>
```

1. [[paso 7]]Verifique los resultados usando el comando:

```
show serviceport
```

```
(cs2)# show serviceport
Interface Status..... Up
IP Address..... 172.19.2.2
Subnet Mask..... 255.255.255.0
Default Gateway..... 172.19.2.254
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is .....
fe80::dac4:97ff:fe71:123c/64
IPv6 Default Router..... fe80::20b:45ff:fea9:5dc0
Configured IPv4 Protocol..... DHCP
Configured IPv6 Protocol..... None
IPv6 AutoConfig Mode..... Disabled
Burned In MAC Address..... D8:C4:97:71:12:3C
```

2. Configure el dominio y el servidor de nombres:

```
ip domain name <domain_name>
ip name server <server_name>
```

```
(cs2)# configure
(cs2) (Config)# ip domain name company.com
(cs2) (Config)# ip name server 10.10.99.1 10.10.99.2
(cs2) (Config)# exit
(cs2)#
```

3. Configure el servidor NTP.

EFOS 3.10.0.3 y posterior

Configure la zona horaria y la sincronización horaria (NTP):

```
sntp server <server_name>
clock
```

```
(cs2)# configure
(cs2) (Config)# ntp server 10.99.99.5
(cs2) (Config)# clock timezone -7
(cs2) (Config)# exit
(cs2)#
```

EFOS 3.9.0.2 y anteriores

Configure la zona horaria y la sincronización horaria (SNTP):

```
sntp client mode <client_mode>
sntp server <server_name>
clock
```

```
(cs2)# configure
(cs2) (Config)# sntp client mode unicast
(cs2) (Config)# sntp server 10.99.99.5
(cs2) (Config)# clock timezone -7
(cs2) (Config)# exit
(cs2)#
```

1. Configure la hora manualmente si no configuró un servidor NTP en el paso anterior.

EFOS 3.10.0.3 y posterior

Configure la hora manualmente.

clock

```
(cs2)# configure
(cs2)(Config)# clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2)(Config)# clock timezone -5 zone EST
(cs2)(Config)# clock set 07:00:00
(cs2)(Config)# clock set 10/20/2023
(cs2)(Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2023
No time source

(cs2)(Config)# exit
(cs2)#
```

EFOS 3.9.0.2 y anteriores

Configure la hora manualmente.

clock

```
(cs2)# configure
(cs2)(Config)# no sntp client mode
(cs2)(Config)# clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2)(Config)# clock timezone -5 zone EST
(cs2)(Config)# clock set 07:00:00
(cs2)(Config)# clock set 10/20/2023
(cs2)(Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2023
No time source

(cs2)(Config)# exit
(cs2)#
```

1. Guardar la configuración en ejecución en la configuración de inicio:

```
write memory
```

```
(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!
```

El futuro

["Instale el software del EFOS"](#).

Instale el software del EFOS

Siga estos pasos para instalar el software Ethernet Fabric OS (EFOS) en el conmutador de clúster BES-53248.

El software EFOS incluye un conjunto de funciones y protocolos de red avanzados para desarrollar sistemas Ethernet e infraestructura IP. Esta arquitectura de software es adecuada para cualquier dispositivo de organización de red que utilice aplicaciones que requieran una inspección o separación exhaustiva de paquetes.

Preparación de la instalación

Antes de empezar

- Este procedimiento solo es adecuado para instalaciones nuevas.
- Descargue el software Broadcom EFOS aplicable para los switches de su clúster de la ["Compatibilidad con switches Ethernet Broadcom"](#) sitio.
- Asegúrese de que el ["El conmutador de clúster BES-53248 está configurado"](#).

Instale el software

Utilice uno de los siguientes métodos para instalar el software EFOS:

- [Método 1: Instalar EFOS](#). Utilizado en la mayoría de los casos.
- [Método 2: Instale EFOS en modo ONIE](#). Se utiliza si una versión de EFOS es compatible con FIPS y la otra versión de EFOS no es compatible con FIPS.

Método 1: Instalar EFOS

Realice los siguientes pasos para instalar el software EFOS.

Pasos

1. Inicie sesión en el puerto de la consola de serie del switch o conéctese mediante SSH.
2. Utilice la `ping` Comando para verificar la conectividad con el servidor que aloja EFOS, licencias y el archivo RCF.

Muestra el ejemplo

En este ejemplo se comprueba que el conmutador está conectado al servidor en la dirección IP 172.19.2.1:

```
(cs2)# ping 172.19.2.1
Ping 172.19.2.1 with 0 bytes of data:

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

3. Descargue el archivo de imagen en el switch.

Consulte la siguiente tabla para obtener información sobre los protocolos de copia admitidos:

Protocolo	Requisitos
Protocolo trivial de transferencia de archivos (TFTP)	Ninguno
Protocolo de transferencia de archivos SSH (SFTP)	Su paquete de software debe admitir una gestión segura
FTP	Se requiere contraseña
XMÓDEM	Ninguno
YMODEM	Ninguno
ZMODEM	Ninguno
Protocolo de copia segura (SCP)	Su paquete de software debe admitir una gestión segura
HTTP	Las transferencias de archivos basadas en CLI se admiten en plataformas seleccionadas cuando hay disponible una utilidad WGET nativa
HTTPS	Las transferencias de archivos basadas en CLI se admiten en plataformas seleccionadas cuando hay disponible una utilidad WGET nativa

Copiar el archivo de imagen en la imagen activa significa que al reiniciar, esa imagen establece la versión EFOS en ejecución. La imagen anterior sigue estando disponible como copia de seguridad.

Muestra el ejemplo

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.10.0.3.stk active
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... EFOS-3.10.0.3.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.
```

4. Mostrar 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         3.7.0.4      3.7.0.4      3.7.0.4              3.10.0.3
```

5. Reinicie el switch:

```
reload
```


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!
```

6. Vuelva a iniciar sesión y compruebe la nueva versión del software EFOS:

```
show version
```

Muestra el ejemplo

```
(cs2)# show version
```

```
Switch: 1
```

```
System Description..... BES-53248A1,  
3.10.0.3, Linux 4.4.211-28a6fe76, 2016.05.00.04  
Machine Type..... BES-53248A1,  
Machine Model..... BES-53248  
Serial Number..... QTFCU38260023  
Maintenance Level..... A  
Manufacturer..... 0xbc00  
Burned In MAC Address..... D8:C4:97:71:0F:40  
Software Version..... 3.10.0.3  
Operating System..... Linux 4.4.211-  
28a6fe76  
Network Processing Device..... BCM56873_A0  
CPLD Version..... 0xff040c03
```

```
Additional Packages..... BGP-4  
..... QOS  
..... Multicast  
..... IPv6  
..... Routing  
..... Data Center  
..... OpEN API  
..... Prototype Open API
```

7. Complete la instalación.
Siga estos cinco pasos para volver a configurar el switch:
 - a. "Instale licencias"
 - b. "Instale el archivo RCF"
 - c. "Habilite SSH"
 - d. "Habilite la recogida de registros"
 - e. "Configure SNMPv3 para la supervisión"
8. Repita los pasos 1 a 7 en el conmutador asociado.

Método 2: Instale EFOS en modo ONIE

Puede realizar los siguientes pasos si una versión de EFOS es compatible con FIPS y la otra versión de EFOS no es compatible con FIPS. Estos pasos se pueden utilizar para instalar la imagen EFOS 3.7.x.x no compatible con FIPS o FIPS desde ONIE si el conmutador no arranca.

Pasos

1. Conéctese a una consola que esté conectada al puerto serie del switch.
2. Arranque el interruptor en el modo DE instalación ONIE.

Durante el arranque, seleccione ONIE cuando vea la solicitud.

Muestra el ejemplo

```
+-----+
|EFOS|
|
| *ONIE
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
+-----+
-+
```

Después de seleccionar **ONIE**, el interruptor se carga y le presenta varias opciones. Seleccione **instalar OS**.

Muestra el ejemplo

```

+-----+
-+
|*ONIE:  Install OS
|
|  ONIE:  Rescue
|
|  ONIE:  Uninstall OS
|
|  ONIE:  Update ONIE
|
|  ONIE:  Embed ONIE
|
|  DIAG:  Diagnostic Mode
|
|  DIAG:  Burn-In Mode
|
|
|
|
|
|
|
|
|
|
+-----+
-+

```

El interruptor se inicia EN el modo DE instalación ONIE.

3. Detenga EL descubrimiento DE ONIE y configure la interfaz Ethernet.

Quando aparecer o seguinte mensagem, pressione **Intro** para invocar a console LA ONIE:

```
Please press Enter to activate this console. Info: eth0:  Checking
link... up.
ONIE:/ #
```



El descubrimiento de ONIE continúa y los mensajes se imprimen en la consola.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

4. Configure la interfaz Ethernet del puerto de gestión del switch y agregue la ruta mediante ifconfig
eth0 <ipAddress> netmask <netmask> up y..route add default gw <gatewayAddress>

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

5. Compruebe que se puede acceder al servidor que aloja el archivo DE instalación ONIE:

ping

Muestra el ejemplo

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

6. Instale el nuevo software del conmutador:

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-installer-x86\_64
```

Muestra el ejemplo

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-
installer-x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http://50.50.50.50/Software/onie-installer-3.7.0.4
...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http://50.50.50.50/Software/onie-
installer-3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

El software se instala y, a continuación, reinicia el conmutador. Deje que el interruptor se reinicie normalmente en la nueva versión de EFOS.

7. Inicie sesión y compruebe que el nuevo software del conmutador está instalado:

```
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      3.7.0.4        3.7.0.4        3.7.0.4         3.10.0.3
(cs2) #
```

8. Complete la instalación.
- El conmutador se reinicia sin aplicar ninguna configuración y se restablece a los valores predeterminados de fábrica. Siga estos seis pasos para volver a configurar el switch:
- "Configurar el switch"
 - "Instale licencias"
 - "Instale el archivo RCF"
 - "Habilite SSH"

- e. ["Habilite la recogida de registros"](#)
- f. ["Configure SNMPv3 para la supervisión"](#)

9. Repita los pasos 1 a 8 en el conmutador asociado.

¿Qué sigue?

["Instale licencias"](#) .

Instale el archivo de configuración de referencia (RCF) y el archivo de licencia

A partir de EFOS 3.12.0.1, puede instalar el archivo de configuración de referencia (RCF) y el archivo de licencia después de configurar el conmutador de cluster BES-53248.



Todos los puertos se configuran al instalar el RCF, pero es necesario instalar la licencia para activar los puertos configurados.

Revise los requisitos

Antes de empezar

Compruebe que los siguientes elementos están en su lugar:

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El RCF actual, disponible en la ["Switches de clúster Broadcom"](#) página.
- Una configuración de inicio en el RCF que refleja las imágenes de inicio deseadas, necesaria si está instalando sólo EFOS y manteniendo su versión actual de RCF. Si necesita cambiar la configuración 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.
- Una conexión de consola al switch, necesaria al instalar el RCF desde un estado predeterminado de fábrica. Este requisito es opcional si ha utilizado el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom manteniendo la conectividad remota"](#) para borrar la configuración, de antemano.

Documentación sugerida

Consulte la tabla de compatibilidad del conmutador para conocer las versiones ONTAP y RCF admitidas. Consulte ["Descarga del software EFOS"](#) página. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis de comandos en el RCF y la que se encuentra en las versiones de EFOS.

Instale el archivo de configuración

Acerca de los ejemplos

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

- Los nombres de los dos interruptores BES-53248 son CS1 y CS2.
- Los nombres de nodo son cluster1-01, cluster1-02, cluster1-03 y cluster1-04.
- Los nombres de LIF de 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.
- En los ejemplos de este procedimiento se utilizan cuatro 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.

Acerca de esta tarea

El procedimiento requiere el uso de comandos de la ONTAP y de comandos del switch de Broadcom; los comandos de la ONTAP se utilizan 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 todos los LIF de clúster al switch de partner operativo mientras realiza los pasos en el switch de destino.



Antes de instalar una nueva versión de software de switch y RCF, utilice el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom manteniendo la conectividad remota"](#). Si debe borrar completamente los ajustes del switch, deberá volver a realizar la configuración básica. Debe estar conectado al switch mediante la consola de serie, ya que el borrado completo de la configuración restablece la configuración de la red de gestión.

Paso 1: Prepare la instalación

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.

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

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

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

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

3. 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                0/2          BES-
53248
          e0b    cs2                0/2          BES-
53248
cluster1-02/cdp
          e0a    cs1                0/1          BES-
53248
          e0b    cs2                0/1          BES-
53248
cluster1-03/cdp
          e0a    cs1                0/4          BES-
53248
          e0b    cs2                0/4          BES-
53248
cluster1-04/cdp
          e0a    cs1                0/3          BES-
53248
          e0b    cs2                0/3          BES-
53248
cluster1::*>
```

4. 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

```
Node: cluster1-04
```

```
Ignore
```

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

b. 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
```

	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	e0b true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			

5. Compruebe que el clúster muestra información para ambos switches de clúster.

ONTAP 9.8 y posteriores

A partir de ONTAP 9.8, utilice el comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 y anteriores

Para ONTAP 9.7 y versiones anteriores, utilice el comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

1. deshabilite la reversión automática en las LIF del clúster.

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

Paso 2: Configurar puertos

1. En el switch CS2, confirme la lista de puertos conectados a los nodos del clúster.

```
show isdp neighbor
```

2. En el switch de clúster cs2, apague los puertos conectados a los puertos del clúster de los nodos. Por ejemplo, si los puertos 0/1 a 0/16 se conectan a los nodos ONTAP:

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

3. Comprobar que las LIF del clúster han migrado a los puertos alojados en el switch del clúster cs1. 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		
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
```

5. Si todavía no lo ha hecho, guarde la configuración del switch actual copiando el resultado del siguiente comando en un archivo de registro:

```
show running-config
```

6. 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 conmutador mediante la consola serie para borrar la configuración del conmutador. Este requisito es opcional si ha utilizado el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom mientras se mantiene la conectividad remota"](#) para borrar la configuración, de antemano.



Borrar la configuración no se eliminan las licencias.

- a. SSH en el switch.

Solo proceda cuando todas las LIF de clúster se hayan eliminado de los puertos del switch y el switch esté preparado para borrar la configuración.

- b. Introduzca el modo de privilegio:

```
(cs2)> enable
(cs2)#
```

- c. Copie y pegue los siguientes comandos para eliminar la configuración anterior de RCF (dependiendo de la versión anterior de RCF utilizada, algunos comandos pueden generar un error si no hay una configuración concreta):

```
clear config interface 0/1-0/56
y
clear config interface lag 1
y
```



```

configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no policy-map InShared
no policy-map InMetroCluster
no policy-map InCluster
no policy-map InClusterRdma
no class-map CLUSTER
no class-map HA
no class-map RDMA
no class-map c5
no class-map c4
no class-map CLUSTER
no class-map CLUSTER_RDMA
no class-map StorageSrc
no class-map StorageDst
no class-map RdmaSrc
no class-map RdmaDst
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit

```

d. Guarde la configuración en ejecución en la configuración de inicio:

```
(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!

e. Reinicie el conmutador:

```
(cs2)# reload
```

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

f. Vuelva a iniciar sesión en el switch usando SSH para completar la instalación de RCF.

7. Registre las personalizaciones realizadas en el RCF anterior y aplíquelas al nuevo RCF. Por ejemplo, configurar las velocidades de los puertos o el modo FEC de codificación fija.
8. Copie el RCF en el bootflash del switch CS2 usando uno de los siguientes protocolos de transferencia: FTP, HTTP, TFTP, SFTP o SCP.

Este ejemplo muestra HTTP que se está utilizando para copiar un RCF al bootflash en el switch CS2:

Muestra el ejemplo

```
(cs2)# copy http://<ip-to-webserver>/path/to/BES-53248-RCF-v1.12-Cluster-HA.txt nvram:reference-config

Mode..... HTTP
Set Server IP..... 172.19.2.1
Path..... <ip-to-
webserver>/path/to/
Filename..... BES-53248-RCF-v1.12-Cluster-HA.txt
Data Type..... Unknown

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...
HTTP Unknown file type transfer starting...
Validating configuration script.....
Configuration script validated.
File transfer operation completed successfully.
```

9. Compruebe que el script se ha descargado y guardado con el nombre de archivo que le ha proporcionado:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
Reference-config.scr 21:54:22	2680	2024 05 31

```
1 configuration script(s) found.
2045 Kbytes free.
```

10. Aplique el script al conmutador:

```
script apply
```

Muestra el ejemplo

```
(cs2)# script apply reference-config.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!
...
...
Configuration script 'reference-config.scr' applied.
```

11. Instale el archivo de licencia.

Muestra el ejemplo

```
(cs2)# copy http://<ip-to-webserver>/path/to/BES-53248-LIC.dat
nvram:license-key 1
Mode..... HTTP
Set Server IP..... 172.19.2.1
Path..... <ip-to-
webserver>/path/to/
Filename..... BES-53248-LIC.dat
Data Type..... license

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...

License Key transfer operation completed successfully.

System reboot is required.
(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!

(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
...
...
```

12. Examine el resultado del banner en `show clibanner` el comando. Debe leer y seguir estas instrucciones para verificar la configuración y el funcionamiento correctos del interruptor.

Muestra el ejemplo

```
(cs2)# show clibanner
```

```
Banner Message configured :
```

```
=====
```

```
BES-53248 Reference Configuration File v1.12 for Cluster/HA/RDMA
```

```
Switch    : BES-53248
```

```
Filename  : BES-53248-RCF-v1.12-Cluster.txt
```

```
Date      : 11-04-2024
```

```
Version   : v1.12
```

```
Port Usage:
```

```
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
```

```
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
```

```
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added  
right to left
```

```
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
```

```
NOTE:
```

- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms of port speed:

- Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44, 45-48

- The port speed should be the same (10GbE or 25GbE) across all ports in a 4-port group

- If additional licenses are purchased, follow the 'Additional Node Ports

- activated with Licenses' section for instructions

- If SSH is active, it will have to be re-enabled manually after 'erase startup-config'

- command has been executed and the switch rebooted"

13. En el switch, compruebe que los puertos adicionales con licencia aparecen después de aplicar el RCF:

```
show port all | exclude Detach
```

Muestra el ejemplo

```
(cs2)# show port all | exclude Detach
```

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					

0/1		Enable	Auto		Down	Enable
Enable long						
0/2		Enable	Auto		Down	Enable
Enable long						
0/3		Enable	Auto		Down	Enable
Enable long						
0/4		Enable	Auto		Down	Enable
Enable long						
0/5		Enable	Auto		Down	Enable
Enable long						
0/6		Enable	Auto		Down	Enable
Enable long						
0/7		Enable	Auto		Down	Enable
Enable long						
0/8		Enable	Auto		Down	Enable
Enable long						
0/9		Enable	Auto		Down	Enable
Enable long						
0/10		Enable	Auto		Down	Enable
Enable long						
0/11		Enable	Auto		Down	Enable
Enable long						
0/12		Enable	Auto		Down	Enable
Enable long						
0/13		Enable	Auto		Down	Enable
Enable long						
0/14		Enable	Auto		Down	Enable
Enable long						
0/15		Enable	Auto		Down	Enable
Enable long						
0/16		Enable	Auto		Down	Enable
Enable long						
0/49		Enable	40G Full		Down	Enable
Enable long						
0/50		Enable	40G Full		Down	Enable
Enable long						

0/51	Enable	100G Full	Down	Enable
Enable long				
0/52	Enable	100G Full	Down	Enable
Enable long				
0/53	Enable	100G Full	Down	Enable
Enable long				
0/54	Enable	100G Full	Down	Enable
Enable long				
0/55	Enable	100G Full	Down	Enable
Enable long				
0/56	Enable	100G Full	Down	Enable
Enable long				

14. En el interruptor, compruebe que se han realizado los cambios:

```
show running-config
```

```
(cs2)# show running-config
```

15. Guarde la configuración en ejecución para que se convierta en la configuración de inicio al reiniciar el conmutador:

```
write memory
```

```
(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!
```

16. Reinicie el conmutador y compruebe que la configuración en ejecución es correcta:

```
reload
```



```
(cs2)# reload
```

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

```
System will now restart!
```

17. En el switch de clúster CS2, saque los puertos conectados a los puertos de clúster de los nodos. Por ejemplo, si los puertos 0/1 a 0/16 se conectan a los nodos ONTAP:

```
(cs2)> enable
```

```
(cs2)# configure
```

```
(cs2) (Config)# interface 0/1-0/16
```

```
(cs2) (Interface 0/1-0/16)# no shutdown
```

```
(cs2) (Interface 0/1-0/16)# exit
```

```
(cs2) (Config)#
```

18. Compruebe los puertos del switch CS2:

```
show interfaces status all | exclude Detach
```

Muestra el ejemplo

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

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

a. Compruebe que los puertos e0b estén activos y en buen estado 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

cluster1-01/cdp	e0a	cs1	0/2
BES-53248	e0b	cs2	0/2
BES-53248			
cluster01-2/cdp	e0a	cs1	0/1
BES-53248	e0b	cs2	0/1
BES-53248			
cluster01-3/cdp	e0a	cs1	0/4
BES-53248	e0b	cs2	0/4
BES-53248			
cluster1-04/cdp	e0a	cs1	0/3
BES-53248	e0b	cs2	0/2
BES-53248			

20. Compruebe que el clúster muestra información para ambos switches de clúster.

ONTAP 9.8 y posteriores

A partir de ONTAP 9,8, utilice el comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 y anteriores

Para ONTAP 9,7 y versiones anteriores, utilice el comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

1. En el switch de cluster CS1, apague los puertos conectados a los puertos de cluster de los nodos.

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

```
(cs1)> enable
(cs1)# configure
(cs1)(Config)# interface 0/1-0/16
(cs1)(Interface 0/1-0/16)# shutdown
```

2. 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

```

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

Cluster					
		cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01		e0a	false		
		cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01		e0b	true		
		cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02		e0a	false		
		cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02		e0b	true		
		cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03		e0a	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		e0a	false		
		cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04		e0b	true		

```

cluster1::*>

```

3. 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. Repita los pasos 4 a 19 en el interruptor CS1.

5. Habilite la reversión automática en las LIF del clúster:

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

6. Reinicie el interruptor CS1. Esto activa las LIF del clúster para que reviertan a sus puertos iniciales. Es posible ignorar los eventos de “puertos de clúster inactivos” que se informan en los nodos mientras se reinicia el switch.

```
(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!
```

Paso 3: Verificar la configuración

1. En el switch CS1, verifique que los puertos del switch conectados a los puertos del cluster sean **UP**:

```
show interfaces status all | exclude Detach
```

Muestra el ejemplo

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

2. Compruebe que el ISL entre los switches CS1 y CS2 funciona:

```
show port-channel 1/1
```

Muestra el ejemplo

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr      Device/      Port      Port
Ports    Timeout      Speed     Active
-----  -
0/55     actor/long      Auto      True
         partner/long
0/56     actor/long      Auto      True
         partner/long
```

3. 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	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

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

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

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

Packet	Source	Destination
Node	Date	LIF
Loss		

cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster01-
02_clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster01-
02_clus2 none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-02_clus2
none		

Todos los lanzamientos de ONTAP

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is 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 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 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)

```

1. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

2. 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
```

El futuro

"Habilite SSH".

Instale licencias para switches de clúster BES-53248

El modelo base de switch de clúster BES-53248 tiene licencia para 16 puertos de 10 GbE o 25 GbE y dos puertos de 100 GbE. Puede añadir puertos nuevos si compra más licencias.



Para EFOS 3,12 y posterior, siga los pasos de instalación en ["Instale el archivo de configuración de referencia \(RCF\) y el archivo de licencia"](#).

Revisar las licencias disponibles

Las siguientes licencias están disponibles para su uso en el conmutador de clúster BES-53248:

Tipo de licencia	Detalles de licencia	Versión de firmware admitida
SW-BES-53248A2-8P-2P	Clave de licencia Broadcom 8PT-10G25G + 2PT-40G100G, X190005/R	EFOS 3.4.4.6 y posterior
SW-BES-53248A2-8P-1025G	Clave de licencia 10G25G de 8 puertos Broadcom, X190005/R	EFOS 3.4.4.6 y posterior
SW-BES53248A2-6P-40-100G	Clave de licencia de Broadcom 6 puertos 40G100G, X190005/R	EFOS 3.4.4.6 y posterior

Licencias heredadas

En la siguiente tabla se enumeran las licencias heredadas que estaban disponibles para su uso en el conmutador de clúster BES-53248:

Tipo de licencia	Detalles de licencia	Versión de firmware admitida
SW-BES-53248A1-G1-8P-LIC	Clave de licencia Broadcom 8P 10-25,2P40-100, X190005/R.	EFOS 3.4.3.3 y posterior
SW-BES-53248A1-G1-16P-LIC	Clave de licencia Broadcom 16P 10-25,4P40-100, X190005/R.	EFOS 3.4.3.3 y posterior

Tipo de licencia	Detalles de licencia	Versión de firmware admitida
SW-BES-53248A1-G1-24P-LIC	Clave de licencia Broadcom 24P 10-25,6P40-100, X190005/R.	EFOS 3.4.3.3 y posterior
SW-BES54248-40-100G-LIC	Clave de licencia Broadcom 6Port 40G100G, X190005/R.	EFOS 3.4.4.6 y posterior
SW-BES53248-8P-10G25G-LIC	Clave de licencia Broadcom de 8 puertos 10G25G, X190005/R.	EFOS 3.4.4.6 y posterior
SW-BES53248-16P-1025G-LIC	Clave de licencia Broadcom 16Port 10G25G, X190005/R.	EFOS 3.4.4.6 y posterior
SW-BES53248-24P-1025G-LIC	Clave de licencia Broadcom 24Port 10G25G, X190005/R.	EFOS 3.4.4.6 y posterior



No se requiere una licencia para la configuración base.

Instale los archivos de licencia

Siga estos pasos para instalar licencias para switches de clúster BES-53248.

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 EFOS, licencias y el archivo RCF.

Muestra el ejemplo

En este ejemplo se comprueba que el conmutador está conectado 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. Compruebe el uso actual de la licencia en el conmutador cs2:

```
show license
```


Muestra el ejemplo

```
(cs2)# show license
Reboot needed..... No
Number of active licenses..... 0

License Index  License Type      Status
-----
No license file found.
```

4. Instale el archivo de licencia.

Repita este paso para cargar más licencias y usar diferentes números de índice de claves.

Muestra el ejemplo

En el siguiente ejemplo, se usa SFTP para copiar un archivo de licencia en un índice de claves 1.

```
(cs2)# copy sftp://root@172.19.2.1/var/lib/tftpboot/license.dat
nvram:license-key 1
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... /var/lib/tftpboot/
Filename..... license.dat
Data Type..... license

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...

License Key transfer operation completed successfully. System reboot
is required.
```

5. Mostrar toda la información de licencia actual y anotar el estado de la licencia antes de reiniciar el conmutador cs2:

```
show license
```

Muestra el ejemplo

```
(cs2)# show license
```

```
Reboot needed..... Yes
```

```
Number of active licenses..... 0
```

License Index	License Type	Status
1	Port	License valid but not applied

6. Mostrar todos los puertos con licencia:

```
show port all | exclude Detach
```

Los puertos de los archivos de licencia adicionales no se muestran hasta que se haya reiniciado el conmutador.

Muestra el ejemplo



```
(cs2)# show port all | exclude Detach
```

Actor		Admin	Physical	Physical	Link	Link	LACP
Intf	Type	Mode	Mode	Status	Status	Trap	Mode
Timeout							
-----	-----	-----	-----	-----	-----	-----	
0/1		Disable	Auto		Down	Enable	
Enable long							
0/2		Disable	Auto		Down	Enable	
Enable long							
0/3		Disable	Auto		Down	Enable	
Enable long							
0/4		Disable	Auto		Down	Enable	
Enable long							
0/5		Disable	Auto		Down	Enable	
Enable long							
0/6		Disable	Auto		Down	Enable	
Enable long							
0/7		Disable	Auto		Down	Enable	
Enable long							
0/8		Disable	Auto		Down	Enable	
Enable long							
0/9		Disable	Auto		Down	Enable	
Enable long							
0/10		Disable	Auto		Down	Enable	
Enable long							
0/11		Disable	Auto		Down	Enable	
Enable long							
0/12		Disable	Auto		Down	Enable	
Enable long							
0/13		Disable	Auto		Down	Enable	
Enable long							
0/14		Disable	Auto		Down	Enable	
Enable long							
0/15		Disable	Auto		Down	Enable	
Enable long							
0/16		Disable	Auto		Down	Enable	
Enable long							
0/55		Disable	Auto		Down	Enable	
Enable long							
0/56		Disable	Auto		Down	Enable	
Enable long							

7. Reinicie el switch:

```
reload
```

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

8. Compruebe que la nueva licencia está activa y tenga en cuenta que se ha aplicado:

```
show license
```

Muestra el ejemplo

```
(cs2)# show license

Reboot needed..... No
Number of installed licenses..... 1
Total Downlink Ports enabled..... 16
Total Uplink Ports enabled..... 8

License Index  License Type                Status
-----
-----
1              Port                    License applied
```

9. Compruebe que todos los puertos nuevos estén disponibles:

```
show port all | exclude Detach
```

Muestra el ejemplo

```
(cs2)# show port all | exclude Detach
```

Actor		Admin	Physical	Physical	Link	Link	LACP
Intf	Type	Mode	Mode	Status	Status	Trap	Mode
Timeout							
-----		-----	-----	-----	-----	-----	
0/1		Disable	Auto		Down	Enable	
Enable long							
0/2		Disable	Auto		Down	Enable	
Enable long							
0/3		Disable	Auto		Down	Enable	
Enable long							
0/4		Disable	Auto		Down	Enable	
Enable long							
0/5		Disable	Auto		Down	Enable	
Enable long							
0/6		Disable	Auto		Down	Enable	
Enable long							
0/7		Disable	Auto		Down	Enable	
Enable long							
0/8		Disable	Auto		Down	Enable	
Enable long							
0/9		Disable	Auto		Down	Enable	
Enable long							
0/10		Disable	Auto		Down	Enable	
Enable long							
0/11		Disable	Auto		Down	Enable	
Enable long							
0/12		Disable	Auto		Down	Enable	
Enable long							
0/13		Disable	Auto		Down	Enable	
Enable long							
0/14		Disable	Auto		Down	Enable	
Enable long							
0/15		Disable	Auto		Down	Enable	
Enable long							
0/16		Disable	Auto		Down	Enable	
Enable long							
0/49		Disable	100G Full		Down	Enable	
Enable long							
0/50		Disable	100G Full		Down	Enable	
Enable long							

0/51	Disable	100G	Full	Down	Enable
Enable long					
0/52	Disable	100G	Full	Down	Enable
Enable long					
0/53	Disable	100G	Full	Down	Enable
Enable long					
0/54	Disable	100G	Full	Down	Enable
Enable long					
0/55	Disable	100G	Full	Down	Enable
Enable long					
0/56	Disable	100G	Full	Down	Enable
Enable long					



Al instalar licencias adicionales, debe configurar las nuevas interfaces manualmente. No vuelva a aplicar un RCF a un interruptor de producción en funcionamiento existente.

Solucione problemas de instalación

Cuando se produzcan problemas al instalar una licencia, ejecute los siguientes comandos de depuración antes de ejecutar `copy` comando de nuevo.

Comandos de depuración que se utilizarán: `debug transfer y.. debug license`

Muestra el ejemplo

```
(cs2)# debug transfer
Debug transfer output is enabled.
(cs2)# debug license
Enabled capability licensing debugging.
```

Cuando ejecute el `copy` con el `debug transfer y.. debug license` opciones habilitadas, se devuelve la salida del registro.

Muestra el ejemplo

```
transfer.c(3083):Transfer process  key or certificate file type = 43
transfer.c(3229):Transfer process  key/certificate cmd = cp
/mnt/download//license.dat.1 /mnt/fastpath/ >/dev/null 2>&1CAPABILITY
LICENSING :
Fri Sep 11 13:41:32 2020: License file with index 1 added.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Validating hash value
29de5e9a8af3e510f1f16764a13e8273922d3537d3f13c9c3d445c72a180a2e6.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Parsing JSON buffer {
  "license": {
    "header": {
      "version": "1.0",
      "license-key": "964B-2D37-4E52-BA14",
      "serial-number": "QTFCU38290012",
      "model": "BES-53248"
    },
    "description": "",
    "ports": "0+6"
  }
}.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: License data does not
contain 'features' field.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Serial number
QTFCU38290012 matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Model BES-53248
matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Feature not found in
license file with index = 1.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Applying license file
1.
```

Compruebe lo siguiente en la salida de depuración:

- Compruebe que el número de serie coincide con: Serial number QTFCU38290012 matched.
- Compruebe que el modelo del interruptor coincide con: Model BES-53248 matched.
- Compruebe que el índice de licencia especificado no se haya utilizado anteriormente. Cuando ya se utiliza un índice de licencia, se devuelve el siguiente error: License file /mnt/download//license.dat.1 already exists.
- Una licencia de puerto no es una licencia de función. Por lo tanto, se espera la siguiente declaración: Feature not found in license file with index = 1.

Utilice la copia comando para realizar una copia de seguridad de licencias de puerto en el servidor:


```
(cs2) # copy nvram:license-key 1  
scp://<UserName>@<IP_address>/saved_license_1.dat
```



Si necesita degradar el software del conmutador de la versión 3.4.4.6, se eliminarán las licencias. Este es el comportamiento esperado.

Debe instalar una licencia anterior adecuada antes de volver a una versión anterior del software.

Activar puertos con licencia nueva

Para activar los puertos con licencia nueva, debe editar la última versión del RCF y anular el comentario de los detalles del puerto correspondientes.

La licencia predeterminada activa los puertos 0/1 a 0/16 y 0/55 a 0/56, mientras que los puertos recién licenciados estarán entre los puertos 0/17 a 0/54, dependiendo del tipo y el número de licencias disponibles. Por ejemplo, para activar la licencia SW-BES54248-40-100G-LIC, debe anular el comentario de la siguiente sección en el RCF:

Muestra el ejemplo

```
.
.
!
! 2-port or 6-port 40/100GbE node port license block
!
interface 0/49
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/50
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/51
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
```

```
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/52
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/53
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/54
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
```

```
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
.
.
```



Para los puertos de alta velocidad entre 0/49 y 0/54 inclusive, quite el comentario de cada puerto pero sólo descomente una línea **velocidad** en el RCF para cada uno de estos puertos, ya sea: **Velocidad 100G full-duplex** o **velocidad 40G full-duplex** como se muestra en el ejemplo. Para puertos de baja velocidad entre 0/17 y 0/48 incluidos, quite la Marca de comentario de toda la sección de 8 puertos cuando se haya activado una licencia apropiada.

El futuro

["Instalación del archivo de configuración de referencia \(RCF\)"](#) o ["Actualice el RCF"](#).

Instalación del archivo de configuración de referencia (RCF)

Puede instalar el archivo de configuración de referencia (RCF) después de configurar el conmutador de clúster BES-53248 y después de aplicar las nuevas licencias.



Para EFOS 3,12 y posterior, siga los pasos de instalación en ["Instale el archivo de configuración de referencia \(RCF\) y el archivo de licencia"](#).

Revise los requisitos

Antes de empezar

Compruebe que los siguientes elementos están en su lugar:

- 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 RCF actual, disponible en la ["Switches de clúster Broadcom"](#) página.
- Una configuración de inicio en el RCF que refleja las imágenes de inicio deseadas, necesaria si está instalando sólo EFOS y manteniendo su versión actual de RCF. Si necesita cambiar la configuración 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.
- Una conexión de consola al switch, necesaria al instalar el RCF desde un estado predeterminado de fábrica. Este requisito es opcional si ha utilizado el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom manteniendo la conectividad remota"](#) para borrar la configuración, de antemano.

Documentación sugerida

Consulte la tabla de compatibilidad del conmutador para conocer las versiones ONTAP y RCF admitidas. Consulte ["Descarga del software EFOS"](#) página. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis de comandos en el RCF y la que se encuentra en las versiones de EFOS.

Instale el archivo de configuración

Acerca de los ejemplos

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

- Los nombres de los dos interruptores BES-53248 son CS1 y CS2.
- Los nombres de nodo son cluster1-01, cluster1-02, cluster1-03 y cluster1-04.
- Los nombres de LIF de 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.
- En los ejemplos de este procedimiento se utilizan cuatro 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.

Acerca de esta tarea

El procedimiento requiere el uso de comandos de la ONTAP y de comandos del switch de Broadcom; los comandos de la ONTAP se utilizan 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 todos los LIF de clúster al switch de partner operativo mientras realiza los pasos en el switch de destino.



Antes de instalar una nueva versión de software de switch y RCF, utilice el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom manteniendo la conectividad remota"](#). Si debe borrar completamente los ajustes del switch, deberá volver a realizar la configuración básica. Debe estar conectado al switch mediante la consola de serie, ya que el borrado completo de la configuración restablece la configuración de la red de gestión.

Paso 1: Prepare la instalación

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.

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

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

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

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

3. 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                      0/2      BES-
53248
           e0b    cs2                      0/2      BES-
53248
cluster1-02/cdp
           e0a    cs1                      0/1      BES-
53248
           e0b    cs2                      0/1      BES-
53248
cluster1-03/cdp
           e0a    cs1                      0/4      BES-
53248
           e0b    cs2                      0/4      BES-
53248
cluster1-04/cdp
           e0a    cs1                      0/3      BES-
53248
           e0b    cs2                      0/3      BES-
53248
cluster1::*>
```

4. 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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


```
Node: cluster1-04
```

```
Ignore
```

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

```
cluster1::*>
```

b. 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
```

	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	e0b true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			

5. Compruebe que el clúster muestra información para ambos switches de clúster.

ONTAP 9.8 y posteriores

A partir de ONTAP 9,8, utilice el comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 y anteriores

Para ONTAP 9,7 y versiones anteriores, utilice el comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

1. deshabilite la reversión automática en las LIF del clúster.

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

Paso 2: Configurar puertos

1. En el switch CS2, confirme la lista de puertos conectados a los nodos del clúster.

```
show isdp neighbor
```

2. En el switch de clúster cs2, apague los puertos conectados a los puertos del clúster de los nodos. Por ejemplo, si los puertos 0/1 a 0/16 se conectan a los nodos ONTAP:

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

3. Comprobar que las LIF del clúster han migrado a los puertos alojados en el switch del clúster cs1. 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			
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
```

5. Si todavía no lo ha hecho, guarde la configuración del switch actual copiando el resultado del siguiente comando en un archivo de registro:

```
show running-config
```

6. 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 conmutador mediante la consola serie para borrar la configuración del conmutador. Este requisito es opcional si ha utilizado el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom mientras se mantiene la conectividad remota"](#) para borrar la configuración, de antemano.



Borrar la configuración no se eliminan las licencias.

- a. SSH en el switch.

Solo proceda cuando todas las LIF de clúster se hayan eliminado de los puertos del switch y el switch esté preparado para borrar la configuración.

- b. Introduzca el modo de privilegio:

```
(cs2)> enable
(cs2)#
```

- c. Copie y pegue los siguientes comandos para eliminar la configuración anterior de RCF (dependiendo de la versión anterior de RCF utilizada, algunos comandos pueden generar un error si no hay una configuración concreta):

```

clear config interface 0/1-0/56
y
clear config interface lag 1
y
configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no class-map CLUSTER
no class-map HA
no class-map RDMA
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit

```

- d. Guarde la configuración en ejecución en la configuración de inicio:

```
(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!

e. Reinicie el conmutador:

```
(cs2)# reload
```

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

f. Vuelva a iniciar sesión en el switch usando SSH para completar la instalación de RCF.

7. Tenga en cuenta lo siguiente:

- a. Si se han instalado licencias de puerto adicionales en el switch, debe modificar el RCF para configurar los puertos adicionales con licencia. Consulte ["Activar puertos con licencia nueva"](#) para obtener más detalles.
- b. Registre las personalizaciones realizadas en el RCF anterior y aplíquelas al nuevo RCF. Por ejemplo, configurar las velocidades de los puertos o el modo FEC de codificación fija.

EFOS versión 3,12.x y posterior

1. Copie el RCF al bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: HTTP, HTTPS, FTP, TFTP, SFTP o SCP.

Este ejemplo muestra SFTP que se está utilizando para copiar un RCF al bootflash del switch CS2:

```
(cs2)# copy tftp://172.19.2.1/BES-53248-RCF-v1.9-Cluster-HA.txt
nvram:reference-config
Remote Password:**
Mode..... TFTP
Set Server IP..... 172.19.2.1
Path..... /
Filename..... BES-53248_RCF_v1.9-Cluster-HA.txt
Data Type..... Config Script
Destination Filename..... reference-config.scr
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.
```

1. Compruebe que el script se ha descargado y guardado con el nombre de archivo que le ha proporcionado:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name	Size(Bytes)	Date of Modification
reference-config.scr	2680	2024 05 31 21:54:22

2 configuration script(s) found.
2042 Kbytes free.

2. Aplique el script al conmutador:

```
script apply
```

```
(cs2)# script apply reference-config.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!
```

```
Configuration script 'reference-config.scr' applied.
```

El resto de las versiones de EFOS

1. Copie el RCF al bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: HTTP, HTTPS, FTP, TFTP, SFTP o SCP.

Este ejemplo muestra SFTP que se está utilizando para copiar un RCF al bootflash del switch CS2:

```
(cs2)# copy sftp://172.19.2.1/tmp/BES-53248_RCF_v1.9-Cluster-HA.txt  
nvrn:script BES-53248_RCF_v1.9-Cluster-HA.scr
```

```
Remote Password:**
```

```
Mode..... SFTP
```

```
Set Server IP..... 172.19.2.1
```

```
Path..... //tmp/
```

```
Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.txt
```

```
Data Type..... Config Script
```

```
Destination Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.scr
```

```
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.
```

1. Compruebe que la secuencia de comandos se ha descargado y guardado en el nombre de archivo que le ha proporcionado:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
----- -----	-----	
BES-53248_RCF_v1.9-Cluster-HA.scr 05:41:00	2241	2020 09 30

```
1 configuration script(s) found.
```

2. Aplique el script al conmutador:

```
script apply
```

```
(cs2)# script apply BES-53248_RCF_v1.9-Cluster-HA.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!
```

```
Configuration script 'BES-53248_RCF_v1.9-Cluster-HA.scr' applied.
```

1. Examine el resultado del banner en `show clibanner` el comando. Debe leer y seguir estas instrucciones para verificar la configuración y el funcionamiento correctos del interruptor.

Muestra el ejemplo

```
(cs2)# show clibanner
```

```
Banner Message configured :
```

```
=====
```

```
BES-53248 Reference Configuration File v1.9 for Cluster/HA/RDMA
```

```
Switch    : BES-53248
```

```
Filename   : BES-53248-RCF-v1.9-Cluster.txt
```

```
Date       : 10-26-2022
```

```
Version    : v1.9
```

```
Port Usage:
```

```
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
```

```
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
```

```
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added  
right to left
```

```
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
```

```
NOTE:
```

```
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms  
of port
```

```
speed:
```

```
Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-  
40, 41-44,  
45-48
```

```
The port speed should be the same (10GbE or 25GbE) across all ports  
in a 4-port
```

```
group
```

```
- If additional licenses are purchased, follow the 'Additional Node  
Ports
```

```
activated with Licenses' section for instructions
```

```
- If SSH is active, it will have to be re-enabled manually after  
'erase
```

```
startup-config'
```

```
command has been executed and the switch rebooted
```

2. En el switch, compruebe que los puertos adicionales con licencia aparecen después de aplicar el RCF:

```
show port all | exclude Detach
```

Muestra el ejemplo

```
(cs2)# show port all | exclude Detach
```

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					

0/1		Enable	Auto		Down	Enable
Enable long						
0/2		Enable	Auto		Down	Enable
Enable long						
0/3		Enable	Auto		Down	Enable
Enable long						
0/4		Enable	Auto		Down	Enable
Enable long						
0/5		Enable	Auto		Down	Enable
Enable long						
0/6		Enable	Auto		Down	Enable
Enable long						
0/7		Enable	Auto		Down	Enable
Enable long						
0/8		Enable	Auto		Down	Enable
Enable long						
0/9		Enable	Auto		Down	Enable
Enable long						
0/10		Enable	Auto		Down	Enable
Enable long						
0/11		Enable	Auto		Down	Enable
Enable long						
0/12		Enable	Auto		Down	Enable
Enable long						
0/13		Enable	Auto		Down	Enable
Enable long						
0/14		Enable	Auto		Down	Enable
Enable long						
0/15		Enable	Auto		Down	Enable
Enable long						
0/16		Enable	Auto		Down	Enable
Enable long						
0/49		Enable	40G Full		Down	Enable
Enable long						
0/50		Enable	40G Full		Down	Enable
Enable long						

0/51	Enable	100G Full	Down	Enable
Enable long				
0/52	Enable	100G Full	Down	Enable
Enable long				
0/53	Enable	100G Full	Down	Enable
Enable long				
0/54	Enable	100G Full	Down	Enable
Enable long				
0/55	Enable	100G Full	Down	Enable
Enable long				
0/56	Enable	100G Full	Down	Enable
Enable long				

3. Compruebe en el conmutador que se han realizado los cambios:

```
show running-config
```

```
(cs2)# show running-config
```

4. Guarde la configuración en ejecución para que se convierta en la configuración de inicio al reiniciar el conmutador:

```
write memory
```

```
(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. Reinicie el conmutador y compruebe que la configuración en ejecución es correcta:

```
reload
```

```
(cs2)# reload
```

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

```
System will now restart!
```

6. En el switch de clúster CS2, saque los puertos conectados a los puertos de clúster de los nodos. Por ejemplo, si los puertos 0/1 a 0/16 se conectan a los nodos ONTAP:

```
(cs2)> enable
```

```
(cs2)# configure
```

```
(cs2) (Config)# interface 0/1-0/16
```

```
(cs2) (Interface 0/1-0/16)# no shutdown
```

```
(cs2) (Interface 0/1-0/16)# exit
```

```
(cs2) (Config)#
```

7. Compruebe los puertos del switch CS2:

```
show interfaces status all | exclude Detach
```

Muestra el ejemplo

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

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

a. Compruebe que los puertos e0b estén activos y en buen estado 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface

cluster1-01/cdp	e0a	cs1	0/2
BES-53248	e0b	cs2	0/2
BES-53248			
cluster01-2/cdp	e0a	cs1	0/1
BES-53248	e0b	cs2	0/1
BES-53248			
cluster01-3/cdp	e0a	cs1	0/4
BES-53248	e0b	cs2	0/4
BES-53248			
cluster1-04/cdp	e0a	cs1	0/3
BES-53248	e0b	cs2	0/2
BES-53248			

9. Compruebe que el clúster muestra información para ambos switches de clúster.

ONTAP 9.8 y posteriores

A partir de ONTAP 9,8, utilice el comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 y anteriores

Para ONTAP 9,7 y versiones anteriores, utilice el comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

1. En el switch de cluster CS1, apague los puertos conectados a los puertos de cluster de los nodos.

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

```
(cs1)> enable
(cs1)# configure
(cs1) (Config)# interface 0/1-0/16
(cs1) (Interface 0/1-0/16)# shutdown
```

2. 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	e0a	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	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	e0a	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
cluster1::*>
```

3. 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. Repita los pasos 4 a 19 en el interruptor CS1.

5. Habilite la reversión automática en las LIF del clúster:

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

6. Reinicie el interruptor CS1. Esto activa las LIF del clúster para que reviertan a sus puertos iniciales. Es posible ignorar los eventos de “puertos de clúster inactivos” que se informan en los nodos mientras se reinicia el switch.

```
(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!
```

Paso 3: Verificar la configuración

1. En el switch CS1, verifique que los puertos del switch conectados a los puertos del cluster sean **UP**:

```
show interfaces status all | exclude Detach
```

Muestra el ejemplo

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

2. Compruebe que el ISL entre los switches CS1 y CS2 funciona:

```
show port-channel 1/1
```


Muestra el ejemplo

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr      Device/      Port      Port
Ports    Timeout      Speed     Active
-----  -
0/55     actor/long      Auto      True
        partner/long
0/56     actor/long      Auto      True
        partner/long
```

3. 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	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

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

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

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

Packet	Source	Destination
Node	Date	LIF
Loss		
-----	-----	-----
-----	-----	-----
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster01-
02_clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster01-
02_clus2 none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-02_clus2
none		

Todos los lanzamientos de ONTAP

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is 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 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 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)

```

1. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

2. 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
```

El futuro

"Habilite SSH".

Habilite SSH en switches de clúster BES-53248

Si utiliza las funciones de recogida de registros y el monitor de estado del switch Ethernet (CSHM), debe generar las claves SSH y, a continuación, habilitar SSH en los switches del clúster.

Pasos

1. Compruebe que SSH está desactivado:

```
show ip ssh
```

Muestra el ejemplo

```
(switch)# show ip ssh

SSH Configuration

Administrative Mode: ..... Disabled
SSH Port: ..... 22
Protocol Level: ..... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA(521)
Key Generation In Progress: ..... None
SSH Public Key Authentication Mode: ..... Disabled
SCP server Administrative Mode: ..... Disabled
```

- Si SSH no está deshabilitado, deshabilítelo de la siguiente manera:

```
no ip ssh server enable
```

```
no ip scp server enable
```



- Para EFOS 3.12 y versiones posteriores, se requiere acceso a la consola ya que las sesiones SSH activas se pierden cuando SSH está deshabilitado.
- Para EFOS 3.11 y versiones anteriores, las sesiones SSH actuales se mantienen abiertas después de deshabilitar el servidor SSH.

+



Asegúrese de deshabilitar SSH antes de modificar las claves, de lo contrario, se informará una advertencia en el conmutador.

2. En el modo de configuración, genere las claves SSH:

```
crypto key generate
```

Muestra el ejemplo

```
(switch)# config

(switch) (Config)# crypto key generate rsa

Do you want to overwrite the existing RSA keys? (y/n): y

(switch) (Config)# crypto key generate dsa

Do you want to overwrite the existing DSA keys? (y/n): y

(switch) (Config)# crypto key generate ecdsa 521

Do you want to overwrite the existing ECDSA keys? (y/n): y
```

3. En el modo de configuración, configure la autorización AAA para la recopilación de registros de ONTAP :

```
aaa authorization commands "noCmdAuthList" none
```

Muestra el ejemplo

```
(switch) (Config)# aaa authorization commands "noCmdAuthList" none
(switch) (Config)# exit
```

4. Vuelva a habilitar SSH/SCP.

Muestra el ejemplo

```
(switch)# ip ssh server enable
(switch)# ip scp server enable
(switch)# ip ssh pubkey-auth
```

5. Guarde estos cambios en la configuración de inicio:

```
write memory
```

Muestra el ejemplo

```
(switch)# 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. Cifrar las claves SSH (solo para **FIPS-mode**):



En el modo FIPS, se requiere que las claves se cifren con una frase de acceso por motivos de seguridad. En ausencia de una clave cifrada, la aplicación no se inicia. Las claves se crean y cifran mediante los siguientes comandos:

Muestra el ejemplo

```
(switch) configure  
(switch) (Config)# crypto key encrypt write rsa passphrase  
<passphrase>
```

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): **y**

Config file 'startup-config' created successfully.

```
(switch) (Config)# crypto key encrypt write dsa passphrase  
<passphrase>
```

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): **y**

Config file 'startup-config' created successfully.

```
(switch) (Config)# crypto key encrypt write ecdsa passphrase  
<passphrase>
```

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): **y**

Config file 'startup-config' created successfully.

```
(switch) (Config)# end  
(switch)# 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!

7. Reinicie el switch:

```
reload
```


8. Compruebe que SSH está habilitado:

```
show ip ssh
```

Muestra el ejemplo

```
(switch)# show ip ssh

SSH Configuration

Administrative Mode: ..... Enabled
SSH Port: ..... 22
Protocol Level: ..... Version 2
SSH Sessions Currently Active: ..... 0
Max SSH Sessions Allowed: ..... 5
SSH Timeout (mins): ..... 5
Keys Present: ..... DSA(1024) RSA(1024)
ECDSA(521)
Key Generation In Progress: ..... None
SSH Public Key Authentication Mode: ..... Enabled
SCP server Administrative Mode: ..... Enabled
```

El futuro

["Configure la supervisión de estado del switch".](#)

Restablecer el conmutador de clúster BES-53248 a los valores predeterminados de fábrica

Para restablecer el conmutador de clúster BES-53248 a los valores predeterminados de fábrica, debe borrar la configuración del conmutador BES-53248.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Cambiar al símbolo del sistema elevado.

```
(cs2)> enable
(cs2)#
```

2. Borrar la configuración de inicio.

```
erase startup-config
```

```
(cs2)# erase startup-config
```

```
Are you sure you want to clear the configuration? (y/n) y
```

3. Reinicie el conmutador.

```
(cs2)# reload
```

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



Si el sistema pregunta si desea guardar la configuración no guardada o modificada antes de volver a cargar el conmutador, seleccione **no**.

1. [[paso 4]] Espere a que el conmutador se recargue y luego inicie sesión en el conmutador.

El usuario predeterminado es “admin” y no se establece ninguna contraseña. Se muestra un símbolo del sistema similar a lo siguiente:

```
(Routing) >
```

Actualizar el conmutador

Flujo de trabajo de actualización para conmutadores de clúster BES-53248

Siga estos pasos para actualizar el software EFOS y los archivos de configuración de referencia (RCF) en los switches de cluster Broadcom BES-54328, según corresponda.

1

"Actualice su versión de EFOS"

Descargue e instale el software Ethernet Fabric OS (EFOS) en el switch de clúster BES-53248.

2

"Actualice su versión de RCF"

Actualice el RCF en el switch de clúster BES-53248 y, a continuación, verifique los puertos para obtener una licencia adicional después de aplicar el RCF.

3

"Compruebe la red del clúster de ONTAP después de actualizar"

Compruebe el estado de la red de cluster ONTAP después de actualizar el software de EFOS o RCF para los switches de cluster BES-53248.

Actualice el software de EFOS

Siga estos pasos para actualizar el software EFOS en el conmutador de cluster BES-

53248.

El software EFOS incluye un conjunto de funciones y protocolos de red avanzados para desarrollar sistemas Ethernet e infraestructura IP. Esta arquitectura de software es adecuada para cualquier dispositivo de organización de red que utilice aplicaciones que requieran una inspección o separación exhaustiva de paquetes.

Prepare la actualización

Antes de empezar

- Descargue el software Broadcom EFOS aplicable para los switches de su clúster de la ["Compatibilidad con switches Ethernet Broadcom"](#) sitio.
- Consulte las siguientes notas sobre las versiones EFOS.

Tenga en cuenta lo siguiente:

- Al actualizar desde EFOS 3.4.x.x a EFOS 3.7.x.x o posterior, el conmutador debe ejecutar EFOS 3.4.4.6 (o posterior versión 3.4.x.x). Si está ejecutando una versión anterior a esa, actualice primero el conmutador a EFOS 3.4.4.6 (o posterior versión 3.4.x.x) y, a continuación, actualice el conmutador a EFOS 3.7.x.x o posterior.
- La configuración para EFOS 3.4.x.x y 3.7.x.x o posterior es diferente. Para cambiar la versión de EFOS de 3.4.x.x a 3.7.x.x o posterior, o viceversa, es necesario restablecer los valores predeterminados de fábrica del conmutador y aplicar los archivos RCF de la versión de EFOS correspondiente. Este procedimiento requiere acceso a través del puerto de la consola de serie.
- A partir de la versión 3.7.x.x de EFOS o posterior, está disponible una versión no compatible con FIPS y compatible con FIPS. Se aplican diferentes pasos al cambiar de una versión que no sea compatible con FIPS a una versión compatible con FIPS o viceversa. Si cambia EFOS de una versión no conforme a FIPS a una versión compatible con FIPS o viceversa, el cambio se restablecerá a los valores predeterminados de fábrica. Este procedimiento requiere acceso a través del puerto de la consola de serie.

Procedimiento	Versión EFOS actual	Nueva versión EFOS	* Pasos de alto nivel*
Pasos para actualizar EFOS entre dos versiones (no compatibles con FIPS) compatibles con FIPS	3.4.x.x.	3.4.x.x.	Actualice la nueva imagen EFOS mediante Método 1: Actualizar EFOS . Se conserva la información de configuración y licencia.

3.4.4.6 (o posterior 3.4.x.x)	3.7.x.x o superior, no conforme a FIPS	Actualice EFOS usando Método 1: Actualizar EFOS . Restablezca el conmutador a los valores predeterminados de fábrica y aplique el archivo RCF para EFOS 3.7.x.x o posterior.	3.7.x.x o superior, no conforme a FIPS
3.4.4.6 (o posterior 3.4.x.x)	Degradar EFOS usando Método 1: Actualizar EFOS . Restablezca el interruptor a los valores predeterminados de fábrica y aplique el archivo RCF para EFOS 3.4.x.x.	3.7.x.x o superior, no conforme a FIPS	
Actualice la nueva imagen EFOS mediante Método 1: Actualizar EFOS . Se conserva la información de configuración y licencia.	3.7.x.x o posterior, conforme a FIPS	3.7.x.x o posterior, conforme a FIPS	Actualice la nueva imagen EFOS mediante Método 1: Actualizar EFOS . Se conserva la información de configuración y licencia.
Pasos para actualizar a/desde una versión de EFOS conforme a FIPS	No conforme a FIPS	Conforme a FIPS	Actualización de la imagen EFOS mediante Método 2: Actualizar EFOS utilizando LA instalación DEL SO . Se perderá la información de licencia y configuración del switch.

Para comprobar si su versión de EFOS cumple con FIPS o no cumple con FIPS, utilice `show fips status` comando. En los siguientes ejemplos, **ip_switch_A1** está utilizando EFOS compatible con FIPS y **ip_switch_A2** está utilizando EFOS no compatible con FIPS.

- En el conmutador IP_SWITCH_A1 (EFOS conforme a FIPS):

IP_switch_a1 # **show fips status**

System running in FIPS mode

- En el conmutador IP_SWITCH_A2 (EFOS no compatible con FIPS):

IP_switch_a2 # **show fips status**

^

% Invalid input detected at ^ marker.

Actualice el software

Utilice uno de los siguientes métodos:

- [Método 1: Actualizar EFOS](#). Para la mayoría de los casos (consulte la tabla anterior).
- [Método 2: Actualizar EFOS utilizando LA instalación DEL SO](#). Se utiliza si una versión de EFOS es compatible con FIPS y la otra versión de EFOS no es compatible con FIPS.



Actualice EFOS en un conmutador a la vez para garantizar el funcionamiento continuo de la red de cluster.

Método 1: Actualizar EFOS

Realice los siguientes pasos para actualizar el software de EFOS.



Tenga en cuenta que después de actualizar los conmutadores de clúster BES-53248 de EFOS 3,3.x.x o 3,4.x.x a EFOS 3.7.0.4 o 3,8.0,2, los enlaces interconmutadores (ISLs) y los canales de puerto se marcan en el estado **Down**. Este es el comportamiento esperado y es seguro continuar con la actualización a menos que esté teniendo problemas con las LIF de reversión automática. Consulte el artículo de la base de conocimientos: "[Error en la actualización NDU del conmutador de clúster BES-53248 a EFOS 3.7.0.4 y posterior](#)" Para obtener más información.

Pasos

1. Conecte el conmutador de clúster BES-53248 a la red de gestión.
2. Utilice la `ping` Comando para verificar la conectividad con el servidor que aloja EFOS, licencias y el archivo RCF.

En este ejemplo se comprueba que el conmutador está conectado 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. Deshabilite la reversión automática en las LIF del clúster.

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

4. Mostrar 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         3.7.0.4      3.4.4.6      3.7.0.4         3.7.0.4
```

5. Descargue el archivo de imagen en el switch.

Copiar el archivo de imagen a la imagen de respaldo significa que cuando reinicia, esa imagen establece la versión de EFOS en ejecución, completando la actualización.

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.10.0.3.stk backup
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... EFOS-3.10.0.3.stk
Data Type..... Code
Destination Filename..... backup

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.
```

6. Mostrar 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         3.7.0.4      3.7.0.4          3.7.0.4          3.10.0.3
```

7. Inicie el sistema desde la configuración de copia de seguridad:

```
boot system backup
```

```
(cs2)# boot system backup
Activating image backup ..
```

8. Mostrar 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	3.10.0.3	3.10.0.3	3.10.0.3	3.10.0.3

9. Guarde la configuración en ejecución en la configuración de inicio:

```
write memory
```

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!

10. Reinicie el switch:

```
reload
```


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!
```

11. Vuelva a iniciar sesión y compruebe la nueva versión del software EFOS:

```
show version
```

Muestra el ejemplo

```
(cs2)# show version
```

```
Switch: 1
```

```
System Description..... BES-53248A1,  
3.10.0.3, Linux 4.4.211-28a6fe76, 2016.05.00.04  
Machine Type..... BES-53248A1,  
Machine Model..... BES-53248  
Serial Number..... QTFCU38260023  
Maintenance Level..... A  
Manufacturer..... 0xbc00  
Burned In MAC Address..... D8:C4:97:71:0F:40  
Software Version..... 3.10.0.3  
Operating System..... Linux 4.4.211-  
28a6fe76  
Network Processing Device..... BCM56873_A0  
CPLD Version..... 0xff040c03
```

```
Additional Packages..... BGP-4  
..... QOS  
..... Multicast  
..... IPv6  
..... Routing  
..... Data Center  
..... OpEN API  
..... Prototype Open API
```

12. Repita los pasos 5 a 11 en el interruptor CS1.
13. Habilite la reversión automática en las LIF del clúster.

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

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

```
network interface show -role Cluster
```

Para obtener información detallada, consulte ["Revierte una LIF a su puerto raíz"](#).

Método 2: Actualizar EFOS utilizando LA instalación DEL SO

Puede realizar los siguientes pasos si una versión de EFOS es compatible con FIPS y la otra versión de EFOS no es compatible con FIPS. Estos pasos se pueden utilizar para actualizar la imagen EFOS 3,7.x.x no compatible con FIPS o FIPS desde ONIE si el switch no arranca.



Esta funcionalidad solo está disponible para EFOS 3.7.x.x o superior, no compatible con FIPS.



Si actualiza EFOS mediante la instalación de ONIE OS, la configuración se restablece a los valores predeterminados de fábrica y se eliminan las licencias. Debe configurar el switch e instalar licencias y un RCF compatible para que el switch vuelva a funcionar con normalidad.

Pasos

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

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

2. Arranque el interruptor en el modo DE instalación ONIE.

Durante el arranque, seleccione ONIE cuando vea el mensaje:

```

+-----+
| EFOS                                     |
| *ONIE                                  |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
+-----+

```

Después de seleccionar **ONIE**, el interruptor se carga y le presenta varias opciones. Seleccione **instalar OS**.

```

+-----+
| *ONIE: Install OS                      |
| ONIE: Rescue                          |
| ONIE: Uninstall OS                    |
| ONIE: Update ONIE                     |
| ONIE: Embed ONIE                      |
| DIAG: Diagnostic Mode                  |
| DIAG: Burn-In Mode                    |
|                                       |
|                                       |
|                                       |
|                                       |
|                                       |
+-----+

```

El interruptor se inicia EN el modo DE instalación ONIE.

3. Detenga EL descubrimiento DE ONIE y configure la interfaz Ethernet.

Cuando aparezca el siguiente mensaje, pulse **Intro** para invocar LA consola ONIE:

```

Please press Enter to activate this console. Info: eth0: Checking
link... up.
ONIE:/ #

```



El descubrimiento de ONIE continúa y los mensajes se imprimen en la consola.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

4. Configure la interfaz Ethernet y agregue la ruta mediante `ifconfig eth0 <ipAddress> netmask <netmask> up` y `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

5. Compruebe que se puede acceder al servidor que aloja el archivo DE instalación ONIE:

ping

Muestra el ejemplo

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

6. Instale el nuevo software del conmutador:

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-installer-x86\_64
```

Muestra el ejemplo

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-
installer-x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http://50.50.50.50/Software/onie-installer-3.7.0.4
...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http://50.50.50.50/Software/onie-
installer-3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

El software se instala y, a continuación, reinicia el conmutador. Deje que el interruptor se reinicie normalmente en la nueva versión de EFOS.

7. Compruebe que el nuevo software del switch está instalado:

```
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       3.7.0.4         3.7.0.4    3.7.0.4         3.10.0.3
(cs2) #
```

8. Complete la instalación. El conmutador se reinicia sin aplicar ninguna configuración y se restablece a los valores predeterminados de fábrica. Lleve a cabo los siguientes pasos para volver a configurar el conmutador:

- a. ["Instale licencias"](#)
- b. ["Instale el RCF"](#)
- c. ["Habilite SSH"](#)
- d. ["Habilite la recogida de registros"](#)

e. ["Configure SNMPv3 para la supervisión"](#)

9. Repita los pasos 2 a 8 en el interruptor CS1.

10. Habilite la reversión automática en las LIF del clúster.

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

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

```
network interface show -role Cluster
```

Para obtener información detallada, consulte ["Revierte una LIF a su puerto raíz"](#).

Actualizar el archivo de configuración de referencia (RCF)

Puede actualizar el archivo de configuración de referencia (RCF) después de actualizar el EFOS del conmutador de clúster BES-53248 y después de aplicar las licencias nuevas.

Antes de empezar

Asegúrese de tener lo siguiente:

- 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 RCF actual, disponible en la ["Switches de clúster Broadcom"](#) página.
- Una configuración de inicio en el RCF que refleja las imágenes de inicio deseadas, necesaria si está instalando sólo EFOS y manteniendo su versión actual de RCF. Si necesita cambiar la configuración 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.
- Una conexión de consola al switch, necesaria al instalar el RCF desde un estado predeterminado de fábrica. Este requisito es opcional si ha utilizado el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom manteniendo la conectividad remota"](#) para borrar la configuración, de antemano.

Documentación sugerida

- Consulte la tabla de compatibilidad del conmutador para conocer las versiones ONTAP y RCF admitidas. Consulte ["Descarga del software EFOS"](#) página. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis de comandos en el RCF y la que se encuentra en las versiones de EFOS.
- Consulte las guías de software y actualización correspondientes disponibles en la ["Broadcom"](#) Sitio para obtener documentación completa sobre los procedimientos de actualización y degradación del conmutador BES-53248.

Acerca de los ejemplos

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

- Los nombres de los dos interruptores BES-53248 son CS1 y CS2.

- Los nombres de nodo son cluster1-01, cluster1-02, cluster1-03 y cluster1-04.
- Los nombres de LIF de 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.
- En los ejemplos de este procedimiento se utilizan cuatro 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.

Acerca de esta tarea

El procedimiento requiere el uso de comandos de la ONTAP y de comandos del switch de Broadcom; los comandos de la ONTAP se utilizan 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 todos los LIF de clúster al switch de partner operativo mientras realiza los pasos en el switch de destino.



Antes de instalar una nueva versión de software de switch y RCF, utilice el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom manteniendo la conectividad remota"](#). Si debe borrar completamente los ajustes del switch, deberá volver a realizar la configuración básica. Debe estar conectado al switch mediante la consola de serie, ya que el borrado de la configuración completa restablece la configuración de la red de gestión.

Paso 1: Prepárese para la actualización

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.

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

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

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

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

3. 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                      0/2      BES-
53248
           e0b    cs2                      0/2      BES-
53248
cluster1-02/cdp
           e0a    cs1                      0/1      BES-
53248
           e0b    cs2                      0/1      BES-
53248
cluster1-03/cdp
           e0a    cs1                      0/4      BES-
53248
           e0b    cs2                      0/4      BES-
53248
cluster1-04/cdp
           e0a    cs1                      0/3      BES-
53248
           e0b    cs2                      0/3      BES-
53248
cluster1::*>
```

4. 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

```
Node: cluster1-04
```

```
Ignore
```

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

```
cluster1::*>
```

b. 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
```

	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	e0b true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			

5. Compruebe que el clúster muestra información para ambos switches de clúster.

ONTAP 9.8 y posteriores

A partir de ONTAP 9,8, utilice el comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 y anteriores

Para ONTAP 9,7 y versiones anteriores, utilice el comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

1. deshabilite la reversión automática en las LIF del clúster.

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

Paso 2: Configurar puertos

1. En el switch CS2, confirme la lista de puertos conectados a los nodos del clúster.

```
show isdp neighbor
```

2. En el switch CS2, apague los puertos conectados a los puertos de clúster de los nodos. Por ejemplo, si los puertos 0/1 a 0/16 se conectan a los nodos ONTAP:

```
(cs2)> enable
(cs2)# configure
(cs2) (Config)# interface 0/1-0/16
(cs2) (Interface 0/1-0/16)# shutdown
(cs2) (Interface 0/1-0/16)# exit
(cs2) (Config)#
```

3. Comprobar que las LIF del clúster han migrado a los puertos alojados en el switch del clúster cs1. 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		

```
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
```

5. Si todavía no lo ha hecho, guarde la configuración del switch actual copiando el resultado del siguiente comando en un archivo de registro:

```
show running-config
```

6. 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 conmutador mediante la consola serie para borrar la configuración del conmutador. Este requisito es opcional si ha utilizado el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión Broadcom mientras se mantiene la conectividad remota"](#) para borrar la configuración, de antemano.



Borrar la configuración no se eliminan las licencias.

- a. SSH en el switch.

Solo proceda cuando todas las LIF de clúster se hayan eliminado de los puertos del switch y el switch esté preparado para borrar la configuración.

- b. Introduzca el modo de privilegio:

```
(cs2)> enable
(cs2)#
```

- c. Copie y pegue los siguientes comandos para eliminar la configuración anterior de RCF (dependiendo de la versión anterior de RCF utilizada, algunos comandos pueden generar un error si no hay una configuración concreta):

```
clear config interface 0/1-0/56
y
clear config interface lag 1
y
```

```

configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no policy-map InShared
no policy-map InMetroCluster
no policy-map InCluster
no policy-map InClusterRdma
no class-map CLUSTER
no class-map HA
no class-map RDMA
no class-map c5
no class-map c4
no class-map CLUSTER
no class-map CLUSTER_RDMA
no class-map StorageSrc
no class-map StorageDst
no class-map RdmaSrc
no class-map RdmaDstA
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit
show running-config

```

d. Guarde la configuración en ejecución en la configuración de inicio:


```
write memory
```

```
(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!
```

e. Reinicie el conmutador:

```
reload
```

```
(cs2)# reload
```

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

a. Vuelva a iniciar sesión en el switch usando SSH para completar la instalación de RCF.

7. Tenga en cuenta lo siguiente:

- a. Si se han instalado licencias de puerto adicionales en el switch, debe modificar el RCF para configurar los puertos adicionales con licencia. Consulte ["Activar puertos con licencia nueva"](#) para obtener más detalles.
- b. Registre las personalizaciones realizadas en el RCF anterior y aplíquelas al nuevo RCF. Por ejemplo, configurar las velocidades de los puertos o el modo FEC de codificación fija.

EFOS versión 3,12.x y posterior

1. Copie el RCF al bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: HTTP, HTTPS, FTP, TFTP, SFTP o SCP.

Este ejemplo muestra SFTP que se está utilizando para copiar un RCF al bootflash del switch CS2:

```
(cs2)# copy sftp://172.19.2.1/BES-53248-RCF-v1.9-Cluster-HA.txt
nvram:reference-config
Remote Password:**
Mode..... TFTP
Set Server IP..... 172.19.2.1
Path..... /
Filename..... BES-53248_RCF_v1.9-
Cluster-HA.txt
Data Type..... Config Script
Destination Filename..... reference-config.scr
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.
```

1. Compruebe que el script se ha descargado y guardado con el nombre de archivo que le ha proporcionado:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name	Size(Bytes)	Date of Modification
reference-config.scr	2680	2024 05 31 21:54:22

2 configuration script(s) found.
2042 Kbytes free.

2. Aplique el script al conmutador:

```
script apply
```

```
(cs2)# script apply reference-config.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!
```

```
Configuration script 'reference-config.scr' applied.
```

El resto de las versiones de EFOS

1. Copie el RCF al bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: HTTP, HTTPS, FTP, TFTP, SFTP o SCP.

Este ejemplo muestra SFTP que se está utilizando para copiar un RCF al bootflash del switch CS2:

```
(cs2)# copy sftp://172.19.2.1/tmp/BES-53248_RCF_v1.9-Cluster-HA.txt  
nvrn:script BES-53248_RCF_v1.9-Cluster-HA.scr
```

```
Remote Password:**
```

```
Mode..... SFTP
```

```
Set Server IP..... 172.19.2.1
```

```
Path..... //tmp/
```

```
Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.txt
```

```
Data Type..... Config Script
```

```
Destination Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.scr
```

```
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.
```

1. Compruebe que la secuencia de comandos se ha descargado y guardado en el nombre de archivo que le ha proporcionado:

```
script list
```

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
----- -----	-----	
BES-53248_RCF_v1.9-Cluster-HA.scr 05:41:00	2241	2020 09 30

```
1 configuration script(s) found.
```

2. Aplique el script al conmutador:

```
script apply
```

```
(cs2)# script apply BES-53248_RCF_v1.9-Cluster-HA.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!
```

```
Configuration script 'BES-53248_RCF_v1.9-Cluster-HA.scr' applied.
```

1. Examine la salida del banner desde el `show clibanner` comando. Debe leer y seguir estas instrucciones para asegurarse de que la configuración y el funcionamiento del interruptor son correctos.

```
show clibanner
```

Muestra el ejemplo

```
(cs2)# show clibanner
```

```
Banner Message configured :
```

```
=====
```

```
BES-53248 Reference Configuration File v1.9 for Cluster/HA/RDMA
```

```
Switch    : BES-53248
```

```
Filename  : BES-53248-RCF-v1.9-Cluster.txt
```

```
Date      : 10-26-2022
```

```
Version   : v1.9
```

```
Port Usage:
```

```
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
```

```
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
```

```
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added  
right to left
```

```
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
```

```
NOTE:
```

```
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms  
of port
```

```
speed:
```

```
Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-  
40, 41-44,  
45-48
```

```
The port speed should be the same (10GbE or 25GbE) across all ports  
in a 4-port
```

```
group
```

```
- If additional licenses are purchased, follow the 'Additional Node  
Ports
```

```
activated with Licenses' section for instructions
```

```
- If SSH is active, it will have to be re-enabled manually after  
'erase
```

```
startup-config'
```

```
command has been executed and the switch rebooted
```

2. En el switch, compruebe que los puertos adicionales con licencia aparecen después de aplicar el RCF:

```
show port all | exclude Detach
```

Muestra el ejemplo

```
(cs2)# show port all | exclude Detach
```

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					

0/1		Enable	Auto		Down	Enable
Enable long						
0/2		Enable	Auto		Down	Enable
Enable long						
0/3		Enable	Auto		Down	Enable
Enable long						
0/4		Enable	Auto		Down	Enable
Enable long						
0/5		Enable	Auto		Down	Enable
Enable long						
0/6		Enable	Auto		Down	Enable
Enable long						
0/7		Enable	Auto		Down	Enable
Enable long						
0/8		Enable	Auto		Down	Enable
Enable long						
0/9		Enable	Auto		Down	Enable
Enable long						
0/10		Enable	Auto		Down	Enable
Enable long						
0/11		Enable	Auto		Down	Enable
Enable long						
0/12		Enable	Auto		Down	Enable
Enable long						
0/13		Enable	Auto		Down	Enable
Enable long						
0/14		Enable	Auto		Down	Enable
Enable long						
0/15		Enable	Auto		Down	Enable
Enable long						
0/16		Enable	Auto		Down	Enable
Enable long						
0/49		Enable	40G Full		Down	Enable
Enable long						
0/50		Enable	40G Full		Down	Enable
Enable long						

0/51	Enable	100G Full	Down	Enable
Enable long				
0/52	Enable	100G Full	Down	Enable
Enable long				
0/53	Enable	100G Full	Down	Enable
Enable long				
0/54	Enable	100G Full	Down	Enable
Enable long				
0/55	Enable	100G Full	Down	Enable
Enable long				
0/56	Enable	100G Full	Down	Enable
Enable long				

3. Compruebe en el interruptor que se han realizado los cambios.

```
show running-config
```

4. Guarde la configuración en ejecución para que se convierta en la configuración de inicio al reiniciar el conmutador:

```
write memory
```

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. Reinicie el conmutador y verifique que la configuración en ejecución sea correcta.

```
reload
```

```
(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
System will now restart!
```

6. En el switch de clúster CS2, saque los puertos conectados a los puertos de clúster de los nodos.

```
(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# no shutdown
(cs2)(Config)# exit
```

7. Guarde la configuración en ejecución en la configuración de inicio:

```
write memory
```

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!
```

8. Compruebe los puertos del switch CS2:

```
show interfaces status all | exclude Detach
```


Muestra el ejemplo

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

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

a. Compruebe que los puertos e0b estén activos y en buen estado 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: cluster1-04

Ignore

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

b. Compruebe el estado del switch del clúster:

```
network device-discovery show
```

Muestra el ejemplo

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

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

cluster1-01/cdp	e0a	cs1	0/2
BES-53248	e0b	cs2	0/2
BES-53248			
cluster01-2/cdp	e0a	cs1	0/1
BES-53248	e0b	cs2	0/1
BES-53248			
cluster01-3/cdp	e0a	cs1	0/4
BES-53248	e0b	cs2	0/4
BES-53248			
cluster1-04/cdp	e0a	cs1	0/3
BES-53248	e0b	cs2	0/2
BES-53248			

10. Compruebe que el clúster muestra información para ambos switches de clúster.

ONTAP 9.8 y posteriores

A partir de ONTAP 9,8, utilice el comando:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2	cluster-network	10.228.143.202	BES-
53248			
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 y anteriores

Para ONTAP 9,7 y versiones anteriores, utilice el comando:

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

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

Switch	Type	Address	Model
cs1 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

1. Repita los pasos 1 a 20 en el interruptor CS1.
2. Habilite la reversión automática en las LIF del clúster:

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

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

```
network interface show -role Cluster
```

Para obtener información detallada, consulte ["Revierte una LIF a su puerto raíz"](#).

Paso 3: Verificar la configuración

1. En el switch CS1, verifique que los puertos del switch conectados a los puertos del cluster sean **UP**:

```
show interfaces status all
```

Muestra el ejemplo

```
(cs1)# show interfaces status all | exclude Detach
```

Media	Flow	Link	Physical	Physical	
Port	Name	State	Mode	Status	Type
Control	VLAN				
-----	-----	-----	-----	-----	
-----	-----	-----			
.					
.					
.					
0/16	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/17	10/25GbE Node Port	Down	Auto		
Inactive	Trunk				
0/18	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
0/19	10/25GbE Node Port	Up	25G Full	25G Full	
25GBase-SR	Inactive Trunk				
.					
.					
.					
0/50	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/51	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/52	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/53	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/54	40/100GbE Node Port	Down	Auto		
Inactive	Trunk				
0/55	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				
0/56	Cluster ISL Port	Up	Auto	100G Full	
Copper	Inactive Trunk				

2. Compruebe que el ISL entre los switches CS1 y CS2 funciona:

```
show port-channel 1/1
```

Muestra el ejemplo

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long      Auto      True
         partner/long
0/56     actor/long      Auto      True
         partner/long
```

3. 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	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0b	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0b	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

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

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

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

Packet	Source	Destination
Node	Date	LIF
Loss		
-----	-----	-----
-----	-----	-----
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster01-
02_clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster01-
02_clus2 none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-02_clus2
none		

Todos los lanzamientos de ONTAP

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is 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 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 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)

```

1. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

2. 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
```

Compruebe la red de cluster ONTAP después de una actualización del software EFOS o RCF de los switches de cluster BES-53248

Puede utilizar los siguientes comandos para verificar el estado de la red de clúster de ONTAP después de una actualización del software EFOS o RCF para los switches de clúster BES-53248.

Pasos

1. Muestra información sobre los puertos de red del clúster con el comando:

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

Link debe tener el valor up y.. Health Status debe ser healthy.

Muestra el ejemplo

En el siguiente ejemplo se muestra el resultado del comando:

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

Node: node1

Ignore

Speed (Mbps) Health

Health

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	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

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

e0a	Cluster	Cluster		up	9000	auto/10000	healthy
false							

e0b	Cluster	Cluster		up	9000	auto/10000	healthy
false							

2. Compruebe esto para cada LIF. Si `Home` es `true` y `Status Admin/Oper` es `up` en ambos nodos, utilizando el comando:

```
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	169.254.217.125/16	node1
e0a	true				
		node1_clus2	up/up	169.254.205.88/16	node1
e0b	true				
		node2_clus1	up/up	169.254.252.125/16	node2
e0a	true				
		node2_clus2	up/up	169.254.110.131/16	node2
e0b	true				

3. Compruebe que el Health Status de cada nodo es true con el comando:

```
cluster show
```

Muestra el ejemplo

```
cluster1::> cluster show
```

Node	Health	Eligibility	Epsilon

node1	true	true	false
node2	true	true	false

El futuro

["Configure la supervisión de estado del switch".](#)

Migrar los switches

Migrar switches de clúster CN1610 a switches de clúster BES-53248

Para migrar los switches de clúster CN1610 de un clúster a switches de clúster BES-53248 compatibles con Broadcom, revise los requisitos de migración y siga el procedimiento de migración.

Se admiten los siguientes switches de clúster:

- CN1610
- BES-53248

Revise los requisitos

Compruebe que la configuración cumple los siguientes requisitos:

- Algunos de los puertos de los conmutadores BES-53248 están configurados para funcionar a 10GbE.
- La conectividad 10GbE desde los nodos a los switches de clúster BES-53248 se ha planificado, migrado y documentado.
- El clúster está funcionando completamente (no debería haber errores en los registros o problemas similares).
- Se ha completado la personalización inicial de los interruptores BES-53248, de modo que:
 - Los conmutadores BES-53248 ejecutan la última versión recomendada del software EFOS.
 - Los archivos de configuración de referencia (RCF) se han aplicado a los conmutadores.
 - La personalización de cualquier sitio, como DNS, NTP, SMTP, SNMP, Y SSH, se configuran en los nuevos switches.

Conexiones de nodos

Los switches de clúster admiten las siguientes conexiones de nodo:

- NetApp CN1610: Puertos 0/1 a 0/12 (10GbE)
- BES-53248: Puertos 0/1-0/16 (10GbE/25GbE)



Los puertos adicionales se pueden activar si se compran licencias de puertos.

Puertos ISL

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

- NetApp CN1610: Puertos 0/13 a 0/16 (10GbE)
- BES-53248: Puertos 0/55-0/56 (100GbE)

La "[Hardware Universe de NetApp](#)" Contiene información acerca de la compatibilidad con ONTAP, el firmware EFOS compatible y el cableado para switches de clúster BES-53248.

Cableado ISL

El cableado ISL adecuado es el siguiente:

- **Principio:** para CN1610 a CN1610 (SFP+ a SFP+), cuatro cables de conexión directa de cobre o fibra óptica SFP+.
- **Final:** para BES-53248 a BES-53248 (QSFP28 a QSFP28), dos transceptores ópticos QSFP28/fibra o cables de conexión directa de cobre.

Migrar los switches

Siga este procedimiento para migrar switches de clúster CN1610 a switches de clúster BES-53248.

Acerca de los ejemplos

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

- En los ejemplos, se utilizan dos nodos, cada uno de los cuales implementa dos puertos de interconexión de clúster de 10 GbE: e0a y.. e0b.
- Los resultados del comando pueden variar en función de las diferentes versiones del software ONTAP.
- Los switches CN1610 que se van a sustituir son CL1 y.. CL2.
- Los switches BES-53248 para reemplazar los switches CN1610 son cs1 y.. cs2.
- Los nodos son node1 y.. node2.
- El interruptor CL2 se sustituye primero por cs2, seguido por CL1 por cs1.
- Los switches BES-53248 están precargados con las versiones compatibles de archivo de configuración de referencia (RCF) y SO Ethernet Fabric (EFOS) con cables ISL conectados en los puertos 55 y 56.
- 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.

Acerca de esta tarea

Este procedimiento cubre el siguiente caso:

- El clúster comienza con dos nodos conectados a dos switches de clúster CN1610.
- El conmutador CN1610 CL2 se sustituye por el conmutador BES-53248 cs2:
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - Desconecte los cables de todos los puertos del clúster de todos los nodos conectados a CL2 y, a continuación, utilice cables admitidos para volver a conectar los puertos al nuevo switch del clúster cs2.
- El conmutador CN1610 CL1 se sustituye por el conmutador BES-53248 cs1:
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - Desconecte los cables de todos los puertos del clúster de todos los nodos conectados a CL1 y, a continuación, utilice cables admitidos para volver a conectar los puertos al nuevo switch del clúster cs1.



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.

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
```

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
```

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

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

Paso 2: Configure los puertos y el cableado

1. En los switches nuevos, confirme que el cableado ISL está en buen estado entre los switches CS1 y CS2:

```
show port-channel
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos ISL están **up** en el switch cs1:

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long      100G Full  True
         partner/long
0/56     actor/long      100G Full  True
         partner/long
(cs1) #
```

El siguiente ejemplo muestra que los puertos ISL están **up** en el conmutador cs2:

```
(cs2)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long      100G Full  True
         partner/long
0/56     actor/long      100G Full  True
         partner/long
```

2. Muestre los puertos de clúster en cada nodo que están conectados a los switches de clúster existentes:

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

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:

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface
node2	/cdp		
	e0a	CL1	0/2
CN1610			
	e0b	CL2	0/2
CN1610			
node1	/cdp		
	e0a	CL1	0/1
CN1610			
	e0b	CL2	0/1
CN1610			

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

a. Verifique que todos los puertos del clúster sean up con un healthy estado:

```
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
Status	Status				Admin/Oper
-----	-----	-----	----	----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e0b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node2

Ignore

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

- b. Compruebe que todas las interfaces del clúster (LIF) están en sus puertos de inicio:

```
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				
	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. Compruebe que el clúster muestra información de ambos switches de clúster:

ONTAP 9.8 y posteriores

A partir de ONTAP 9,8, utilice el comando: `system switch ethernet show -is-monitoring-enabled -enabled-operational true`

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

Switch	Type	Address	Model
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.3.0.3			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.3.0.3			
Version Source: ISDP			

```
cluster1::*>
```

ONTAP 9.7 y anteriores

Para ONTAP 9,7 y versiones anteriores, utilice el comando: `system cluster-switch show -is-monitoring-enabled-operational true`

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

Switch	Type	Address	Model
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.3.0.3			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.3.0.3			
Version Source: ISDP			

```
cluster1::*>
```

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

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

2. En el switch de clúster CL2, apague los puertos conectados a los puertos de clúster de los nodos para conmutar las LIF de clúster:

```
(CL2)# configure
(CL2)(Config)# interface 0/1-0/16
(CL2)(Interface 0/1-0/16)# shutdown
(CL2)(Interface 0/1-0/16)# exit
(CL2)(Config)# exit
(CL2)#
```

3. Compruebe que las LIF del clúster han conmutado al nodo de respaldo a los puertos alojados en el switch del clúster CL1. 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	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0a	false			
	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. 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

- 5. Mueva todos los cables de conexión de nodos de clúster del switch antiguo CL2 al nuevo switch de CS2.
- 6. Confirme el estado de las conexiones de red movidas a CS2:

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


Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

Todos los puertos de clúster que se han movido deben ser up.

7. Compruebe la información de cercanía en los puertos de clúster:

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

Muestra el ejemplo

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

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

node2	/cdp		
	e0a	CL1	0/2
CN1610			
	e0b	cs2	0/2
53248			BES-
node1	/cdp		
	e0a	CL1	0/1
CN1610			
	e0b	cs2	0/1
53248			BES-

8. Confirme que las conexiones de puertos del switch sean correctas desde la perspectiva del switch CS2:

```
cs2# show interface all
cs2# show isdp neighbors
```

9. En el switch de clúster CL1, apague los puertos conectados a los puertos de clúster de los nodos para conmutar las LIF de clúster:

```
(CL1)# configure
(CL1) (Config)# interface 0/1-0/16
(CL1) (Interface 0/1-0/16)# shutdown
(CL1) (Interface 0/13-0/16)# exit
(CL1) (Config)# exit
(CL1) #
```

Todos los LIF del clúster realizan la conmutación al respaldo al switch CS2.

10. Compruebe que los LIF de clúster han conmutado al nodo de respaldo a los puertos alojados en el switch CS2. Esto puede tardar unos segundos:

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

Muestra el ejemplo

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

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

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0b	false			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0b	false			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

11. 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

12. Mueva los cables de conexión de nodo de clúster de CL1 al nuevo switch de CS1.

13. Confirme el estado de las conexiones de red movidas a CS1:

```
network port show -ipSPACE Cluster
```

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

Todos los puertos de clúster que se han movido deben ser up.

14. Compruebe la información de cercanía en los puertos de clúster:

```
network device-discovery show
```

Muestra el ejemplo

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

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

node1	/cdp		
	e0a	cs1	0/1
53248			BES-
	e0b	cs2	0/1
53248			BES-
node2	/cdp		
	e0a	cs1	0/2
53248			BES-
	e0b	cs2	0/2
53248			BES-

15. Confirme que las conexiones de puertos del switch sean correctas desde la perspectiva del switch CS1:

```
cs1# show interface all
cs1# show isdp neighbors
```

16. Compruebe que el ISL entre CS1 y CS2 aún está operativo:

```
show port-channel
```

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos ISL están **up** en el switch cs1:

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long    100G Full  True
         partner/long
0/56     actor/long    100G Full  True
         partner/long
(cs1) #
```

El siguiente ejemplo muestra que los puertos ISL están **up** en el conmutador cs2:

```
(cs2)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long    100G Full  True
         partner/long
0/56     actor/long    100G Full  True
         partner/long
```

17. Elimine los switches CN1610 sustituidos de la tabla de switches del clúster si no se eliminan

automáticamente:

ONTAP 9.8 y posteriores

A partir de ONTAP 9,8, utilice el comando: `system switch ethernet delete -device device-name`

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

ONTAP 9.7 y anteriores

Para ONTAP 9,7 y versiones anteriores, utilice el comando: `system cluster-switch delete -device device-name`

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

Paso 3: Verificar la configuración

1. Habilite la reversión automática en las LIF del clúster.

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

2. Compruebe que las LIF del clúster han vuelto a sus puertos raíz (esto puede tardar un minuto):

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

Si los LIF del clúster no han cambiado a su puerto de inicio, los revierte manualmente:

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

3. Compruebe que el clúster esté en buen estado:

```
cluster show
```

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

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

		Source	Destination
Packet			
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2_clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
none			

Todos los lanzamientos de ONTAP

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

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



```

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

```

1. Si suprimió la creación automática de casos, vuelva a activarla llamando a un mensaje AutoSupport:

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

```

cluster::*> system node autosupport invoke -node * -type all -message
MAINT=END

```

El futuro

"Configure la supervisión de estado del switch".

Migrar a un entorno de clúster de NetApp conmutado

Si tiene un entorno de clúster *sin switch* de dos nodos existente, puede migrar a un entorno de clúster *con switches* de dos nodos mediante switches de clúster BES-53248 compatibles con Broadcom, lo que le permite escalar más allá de dos nodos del clúster.

El proceso de migración funciona para todos los puertos de nodo de clúster que utilizan puertos ópticos o Twinax, pero no es compatible con este switch si los nodos utilizan puertos RJ45 10GBASE-T integrados para los puertos de red de clúster.

Revise los requisitos

Revise los siguientes requisitos para el entorno del clúster.

- Tenga en cuenta que la mayoría de los sistemas requieren dos puertos de red de clúster dedicados en cada controladora.
- Asegúrese de que el conmutador de clúster BES-53248 está configurado como se describe en ["Sustituya los requisitos"](#) antes de iniciar este proceso de migración.
- Para la configuración con dos nodos sin switch, asegúrese de lo siguiente:
 - La configuración sin switch de dos nodos está correctamente configurada y funciona.
 - Los nodos ejecutan ONTAP 9.5P8 y versiones posteriores. La compatibilidad con puertos de clúster de 40/100 GbE comienza con el firmware EFOS versión 3.4.4.6 y 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 de clúster BES-53248 compatible con Broadcom, asegúrese de lo siguiente:
 - El conmutador de clúster BES-53248 es completamente funcional en ambos switches.
 - Ambos switches tienen conectividad de red de gestión.
 - Hay acceso de la consola a los switches de clúster.
 - El switch nodo a nodo BES-53248 y las conexiones de switch a switch utilizan cables Twinax o de fibra.

La ["Hardware Universe de NetApp"](#) Contiene información acerca de la compatibilidad con ONTAP, el firmware EFOS compatible y el cableado para los switches BES-53248.

- Los cables de enlace entre switches (ISL) están conectados a los puertos 0/55 y 0/56 en los dos switches BES-53248.
- Se ha completado la personalización inicial de los dos switches BES-53248, lo que permite lo siguiente:
 - Los switches BES-53248 ejecutan la última versión del software.
 - Los switches BES-53248 tienen licencias de puerto opcionales instaladas, si se han adquirido.
 - Los archivos de configuración de referencia (RCF) se aplican a los conmutadores.
- Cualquier personalización del sitio (SMTP, SNMP y SSH) se configura en los nuevos switches.

Restricciones de velocidad del grupo de puertos

- Los puertos 48 10/25GbE (SFP28/SFP+) se combinan en 12 grupos de 4 puertos de la siguiente manera: Puertos 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44 y 45-48.
- La velocidad del puerto SFP28/SFP+ debe ser la misma (10 GbE o 25 GbE) en todos los puertos del grupo de 4 puertos.
- Si las velocidades de un grupo de 4 puertos son diferentes, los puertos del switch no funcionarán correctamente.

Migre al entorno del clúster

Acerca de los ejemplos

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

- Los nombres de los conmutadores BES-53248 son `cs1` y.. `cs2`.
- Los nombres de las SVM del clúster son `node1` y.. `node2`.
- Los nombres de las LIF son `node1_clus1` y.. `node1_clus2` en el nodo 1, y. `node2_clus1` y.. `node2_clus2` en el nodo 2 respectivamente.
- La `cluster1::*>` prompt indica el nombre del clúster.
- Los puertos de clúster que se utilizan en este procedimiento son `e0a` y.. `e0b`.

La "[Hardware Universe de NetApp](#)" contiene la información más reciente acerca de los puertos del clúster reales para las plataformas.

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
```

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
```

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

```
set -privilege advanced
```

El aviso avanzado (`*>`) aparece.

Paso 2: Configure los puertos y el cableado

1. Desactive todos los puertos activados orientados al nodo (no los puertos ISL) en los nuevos switches de clúster **cs1** y **cs2**.



No debe deshabilitar los puertos ISL.

En el siguiente ejemplo se muestra que los puertos 1 a 16 que están orientados al nodo están deshabilitados en el switch `cs1`:

```
(cs1)# configure  
(cs1) (Config)# interface 0/1-0/16  
(cs1) (Interface 0/1-0/16)# shutdown  
(cs1) (Interface 0/1-0/16)# exit  
(cs1) (Config)# exit
```

2. Compruebe que el ISL y los puertos físicos en el ISL entre los dos switches BES-53248 CS1 y CS2 están activos:

```
show port-channel
```

Muestra el ejemplo

El siguiente ejemplo muestra que los puertos ISL están activos en el switch cs1:

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long    100G Full  True
         partner/long
0/56     actor/long    100G Full  True
         partner/long
(cs1) #
```

El siguiente ejemplo muestra que los puertos ISL están activos en el switch cs2:

```
(cs2)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----  -
0/55     actor/long    100G Full  True
         partner/long
0/56     actor/long    100G Full  True
         partner/long
```

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	0/55	176	R	BES-53248	0/55
cs2	0/56	176	R	BES-53248	0/56

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
cs2	0/55	176	R	BES-53248	0/55
cs2	0/56	176	R	BES-53248	0/56

4. Compruebe que todos los puertos del clúster estén activos:

```
network port show -ip space Cluster
```

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

5. Compruebe que todas las LIF del clúster estén en funcionamiento:

```
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				
e0a	node1_clus1	up/up	169.254.209.69/16	node1
	true			
e0b	node1_clus2	up/up	169.254.49.125/16	node1
	true			
e0a	node2_clus1	up/up	169.254.47.194/16	node2
	true			
e0b	node2_clus2	up/up	169.254.19.183/16	node2
	true			

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

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

7. Desconecte el cable del puerto del clúster e0a del nodo 1 y, a continuación, conecte e0a al puerto 1 del switch del clúster cs1 mediante el cableado adecuado compatible con los switches BES-53248.

La "[Hardware Universe de NetApp](#)" contiene más información sobre el cableado.

8. 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 mediante el cableado adecuado compatible con los switches BES-53248.
9. Habilite todos los puertos orientados al nodo en el switch de clúster cs1.

El siguiente ejemplo muestra que los puertos 1 a 16 están habilitados en el conmutador cs1:

```
(cs1)# configure  
(cs1)(Config)# interface 0/1-0/16  
(cs1)(Interface 0/1-0/16)# no shutdown  
(cs1)(Interface 0/1-0/16)# exit  
(cs1)(Config)# exit
```

10. Compruebe que todos los puertos del clúster estén activos:


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

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

11. Compruebe que todas las LIF del clúster estén en funcionamiento:

```
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
false					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
false					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

12. 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

- 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 BES-53248.
- 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 BES-53248.
- Habilite todos los puertos orientados al nodo en el switch de clúster cs2.

El siguiente ejemplo muestra que los puertos 1 a 16 están habilitados en el conmutador cs2:

```
(cs2)# configure
(cs2) (Config)# interface 0/1-0/16
(cs2) (Interface 0/1-0/16)# no shutdown
(cs2) (Interface 0/1-0/16)# exit
(cs2) (Config)# exit
```

16. Compruebe que todos los puertos del clúster estén activos:

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

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

Paso 3: Verificar la configuración

1. Habilite la reversión automática en las LIF del clúster.

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

2. Compruebe que las LIF del clúster han vuelto a sus puertos raíz (esto puede tardar un minuto):

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

Si los LIF del clúster no han cambiado a su puerto de inicio, los revierte manualmente:

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

3. Compruebe que se muestran todas las interfaces true para Is Home:

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



Esto puede tardar varios minutos en completarse.

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. Compruebe que ambos nodos tengan una conexión cada uno con 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	175	H	FAS2750	e0a
node2	0/2	157	H	FAS2750	e0a
cs2	0/55	178	R	BES-53248	0/55
cs2	0/56	178	R	BES-53248	0/56

```
(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	137	H	FAS2750	e0b
node2	0/2	179	H	FAS2750	e0b
cs1	0/55	175	R	BES-53248	0/55
cs1	0/56	175	R	BES-53248	0/56

5. 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
53248			BES-
	e0b	cs2	0/2
53248			BES-
node1	/cdp		
	e0a	cs1	0/1
53248			BES-
	e0b	cs2	0/1
53248			BES-

6. 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.

La false el resultado del ejemplo siguiente muestra que las opciones de configuración están deshabilitadas:

```
cluster1::*> network options switchless-cluster show
```

Enable Switchless Cluster: false

7. 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

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

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

		Source	Destination
Packet			
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2_clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
none			

Todos los lanzamientos de ONTAP

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

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



```

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

```

1. vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

2. 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
-messsage MAINT=END

```

Para obtener más información, consulte: ["Artículo de la base de conocimientos de NetApp: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#)

El futuro

["Configure la supervisión de estado del switch"](#).

Reemplace los interruptores

Requisitos de sustitución

Antes de sustituir el interruptor, asegúrese de que se cumplen las siguientes condiciones en el entorno actual y en el interruptor de sustitución.

Infraestructura de red y clúster existente

Asegúrese de que:

- El clúster existente se ha verificado como completamente funcional, con al menos un switch de clúster completamente conectado.
- Todos los puertos del clúster son **up**.
- Todas las interfaces lógicas de cluster (LIF) están administrativamente y operativamente **up** y en sus puertos domésticos.
- La `ONTAP cluster ping-cluster -node node1` el comando debe indicar que la configuración, `basic connectivity y..larger than PMTU communication`, se realizan correctamente en todas las rutas.

Conmutador de clúster de sustitución BES-53248

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.
- Las conexiones de nodos son los puertos 0/1 a 0/16 con licencia predeterminada.
- Todos los puertos de enlace entre switches (ISL) están deshabilitados en los puertos 0/55 y 0/56.
- El archivo de configuración de referencia (RCF) y la imagen del conmutador del sistema operativo EFOS se cargan en el conmutador.
- Se ha completado la personalización inicial del conmutador, tal y como se detalla en ["Configure el conmutador de clúster BES-53248"](#).

Cualquier personalización de sitio anterior, como STP, SNMP y SSH, se copian al nuevo switch.

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después de las tareas de mantenimiento para deshabilitar la creación de casos durante el mantenimiento. Consulte este artículo de la base de conocimientos ["SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#) para obtener más detalles.
- Habilite el registro de sesiones para cualquier sesión de CLI. Para obtener instrucciones sobre cómo activar el registro de sesiones, consulte la sección «Salida de sesión de registro» de este artículo de la base de conocimientos ["Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP"](#).

Si quiere más información

- ["Sitio de soporte de NetApp"](#)
- ["Hardware Universe de NetApp"](#)

Sustituya un switch de clúster BES-53248 compatible con Broadcom

Siga estos pasos para sustituir un conmutador de clúster BES-53248 compatible con Broadcom defectuoso en una red de clúster. Este es un procedimiento no disruptivo (NDU).

Acerca de los ejemplos

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

- Los nombres de los conmutadores BES-53248 existentes son `cs1` y.. `cs2`.
- El nombre del nuevo conmutador BES-53248 es `newcs2`.
- Los nombres de nodo son `node1` y.. `node2`.
- Los puertos del clúster de cada nodo se llaman `e0a` y.. `e0b`.
- 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 prompt de cambios en todos los nodos del clúster es `cluster1::>`

Acerca de la topología

Este procedimiento se basa en la siguiente topología de red de clúster:

Mostrar topología de 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							

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
```

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
-----	-----	-----	-----	
node2	/cdp			
	e0a	cs1	0/2	BES-
53248				
	e0b	cs2	0/2	BES-
53248				
node1	/cdp			
	e0a	cs1	0/1	BES-
53248				
	e0b	cs2	0/1	BES-
53248				

```
(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 Port ID	Intf	Holdtime	Capability	Platform
node1 e0a	0/1	175	H	FAS2750
node2 e0a	0/2	152	H	FAS2750
cs2 0/55	0/55	179	R	BES-53248
cs2 0/56	0/56	179	R	BES-53248

```
(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 Port ID	Intf	Holdtime	Capability	Platform
node1 e0b	0/1	129	H	FAS2750
node2 e0b	0/2	165	H	FAS2750
cs1 0/55	0/55	179	R	BES-53248
cs1 0/56	0/56	179	R	BES-53248

Pasos

1. Revise la ["Requisitos de sustitución"](#).
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.

3. Instale el archivo de configuración de referencia (RCF) y la imagen adecuados en el conmutador, newcs2, y realice las preparaciones necesarias del sitio.

Si es necesario, verifique, descargue e instale las versiones adecuadas del software RCF y EFOS para el nuevo conmutador. Si ha comprobado que el nuevo interruptor está correctamente configurado y no necesita actualizaciones para el software RCF y EFOS, continúe con el paso 2.

- a. Puede descargar el software Broadcom EFOS aplicable para los switches de clúster de la ["Compatibilidad con switches Ethernet Broadcom"](#) sitio. Siga los pasos de la página de descarga para descargar el archivo EFOS de la versión del software ONTAP que está instalando.
 - b. El RCF adecuado está disponible en ["Switches de clúster Broadcom"](#) página. Siga los pasos de la página de descarga para descargar el RCF correcto para la versión del software ONTAP que está instalando.
4. En el nuevo switch, inicie sesión como `admin` y apague todos los puertos que se conectarán a las interfaces del clúster de nodos (puertos 1 a 16).



Si ha adquirido licencias adicionales para puertos adicionales, apague estos puertos también.

Si el switch que desea sustituir no está funcional y está apagado, los LIF de los nodos del clúster ya deberían haber realizado una conmutación al otro puerto del clúster para cada nodo.



No se requiere ninguna contraseña para introducirla `enable` modo.

Muestra el ejemplo

```
User: admin
Password:
(newcs2)> enable
(newcs2)# config
(newcs2) (config)# interface 0/1-0/16
(newcs2) (interface 0/1-0/16)# shutdown
(newcs2) (interface 0/1-0/16)# exit
(newcs2) (config)# exit
(newcs2)#
```

5. Compruebe que todas las LIF del clúster tienen `auto-revert` habilitado:

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

Mostrar topología de ejemplo

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

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

6. Apague los puertos ISL 0/55 y 0/56 en el switch BES-53248 cs1:

Mostrar topología de ejemplo

```
(cs1)# config
(cs1)(config)# interface 0/55-0/56
(cs1)(interface 0/55-0/56)# shutdown
```

7. Elimine todos los cables del conmutador BES-53248 cs2 y, a continuación, conéctelos a los mismos puertos del conmutador BES-53248 newcs2.
8. Traiga los puertos ISL 0/55 y 0/56 entre los switches cs1 y newcs2 y, a continuación, verifique el estado de operación del canal de puerto.

El estado de enlace para el canal de puerto 1/1 debe ser **up** y todos los puertos miembros deben ser True bajo el encabezado Port Active.

Muestra el ejemplo

En este ejemplo, se habilitan los puertos ISL 0/55 y 0/56, y se muestra el estado de enlace para el canal de puerto 1/1 en el switch cs1:

```
(cs1)# config
(cs1)(config)# interface 0/55-0/56
(cs1)(interface 0/55-0/56)# no shutdown
(cs1)(interface 0/55-0/56)# exit
(cs1)# show port-channel 1/1
```

Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr	Device/ Ports	Port Timeout	Port Speed	Port Active
-----	-----	-----	-----	-----
0/55	actor/long partner/long	100G Full	True	
0/56	actor/long partner/long	100G Full	True	

9. En el nuevo switch newcs2, vuelva a habilitar todos los puertos conectados a las interfaces de clúster del nodo (puertos 1 a 16).



Si ha adquirido licencias adicionales para puertos adicionales, apague estos puertos también.

Muestra el ejemplo

```
User:admin
Password:
(newcs2)> enable
(newcs2)# config
(newcs2) (config)# interface 0/1-0/16
(newcs2) (interface 0/1-0/16)# no shutdown
(newcs2) (interface 0/1-0/16)# exit
(newcs2) (config)# exit
```

10. Compruebe que el puerto e0b está **activo**:

```
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						

11. En el mismo nodo que haya utilizado en el paso anterior, espere a que la LIF del clúster no1_clus2 del nodo 1 se revierte automáticamente.

Muestra el ejemplo

En este ejemplo, la LIF no1_clus2 del nodo 1 se revierte correctamente si Is Home es true y el puerto es e0b.

El siguiente comando muestra información acerca de las LIF en ambos nodos. El estado del primer nodo es correcto si Is Home es true en ambas interfaces de clúster y muestran las asignaciones de puerto correctas, en este ejemplo e0a y.. e0b en el nodo 1.

```
cluster::> 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			

12. Muestra información sobre los nodos de un clúster:

```
cluster show
```

Muestra el ejemplo

En este ejemplo se muestra el estado del nodo para node1 y.. node2 en este clúster lo es true:

```
cluster1::> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	true
node2	true	true	true

13. Confirme la siguiente configuración de red del clúster:

```
network port show
```

```
network interface 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					

```
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.
```

14. Compruebe que la red de clúster esté en buen estado:

```
show isdp neighbors
```

Muestra el ejemplo

```
(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	175	H	FAS2750	e0a
node2	0/2	152	H	FAS2750	e0a
newcs2	0/55	179	R	BES-53248	0/55
newcs2	0/56	179	R	BES-53248	0/56

```
(newcs2)# 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	129	H	FAS2750	e0b
node2	0/2	165	H	FAS2750	e0b
cs1	0/55	179	R	BES-53248	0/55
cs1	0/56	179	R	BES-53248	0/56

15. 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
```

El futuro

"Configure la supervisión de estado del switch".

Sustituya los switches del clúster Broadcom BES-53248 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.

Antes de empezar

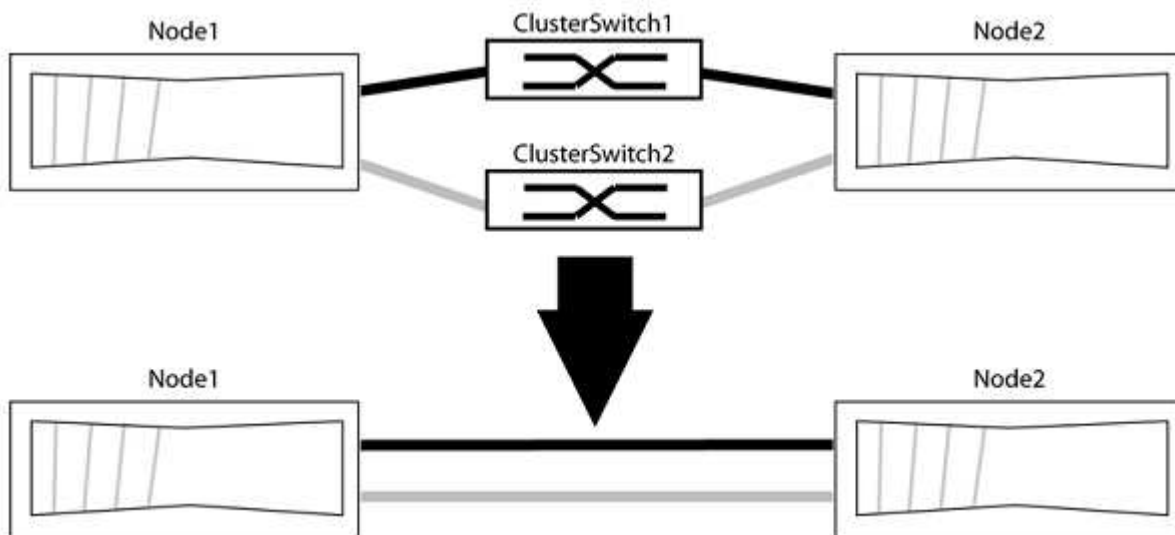
Asegúrese de tener lo siguiente:

- 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

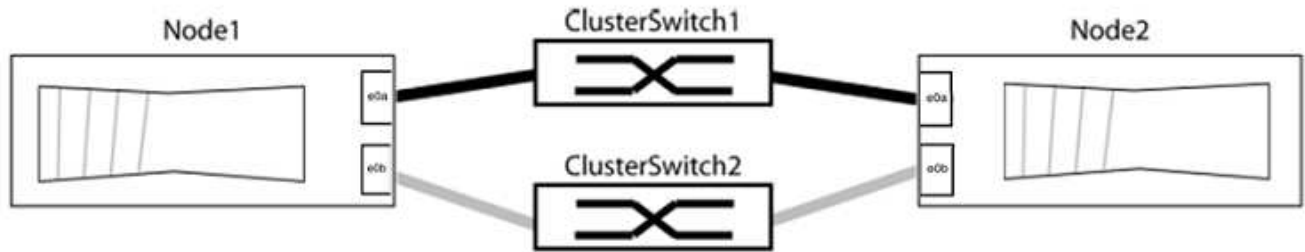
```
cluster::*> system node autosupport invoke -node * -type all
-messsage MAINT=2h
```

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 de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

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

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

```

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

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

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Verifique que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

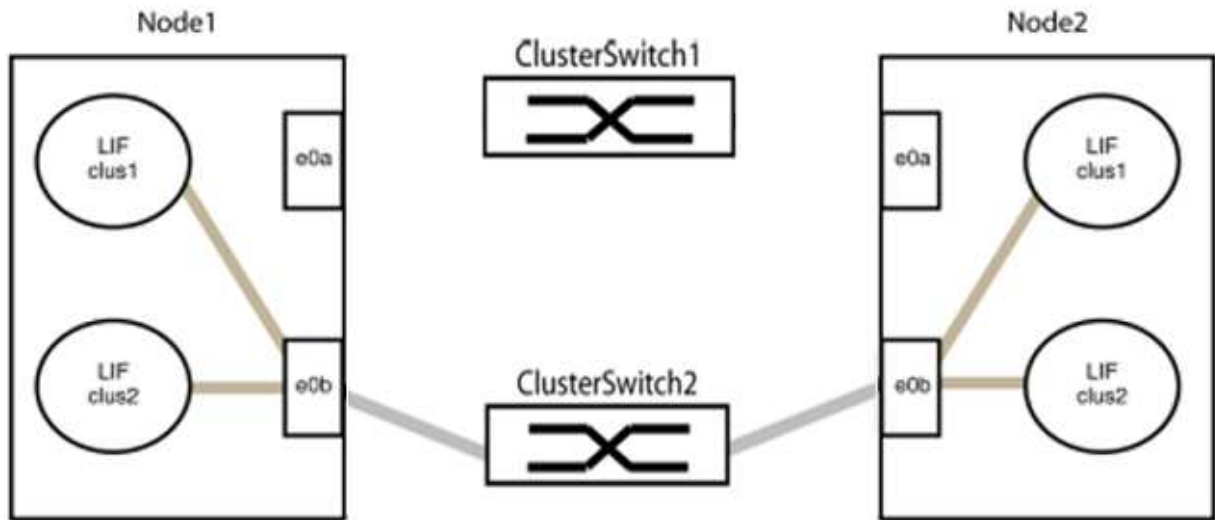
2. Configure la configuración sin switches para los puertos del grupo 1.



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**.

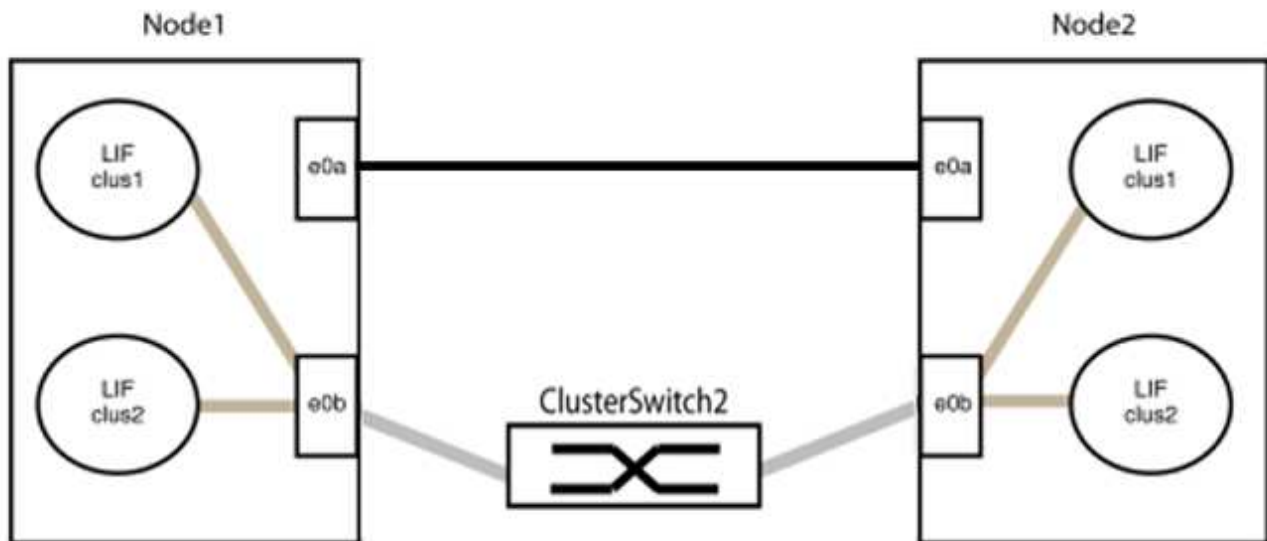
- a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

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:



3. 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
```

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

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

Todos los lanzamientos de ONTAP

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

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

```

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

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

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```



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.

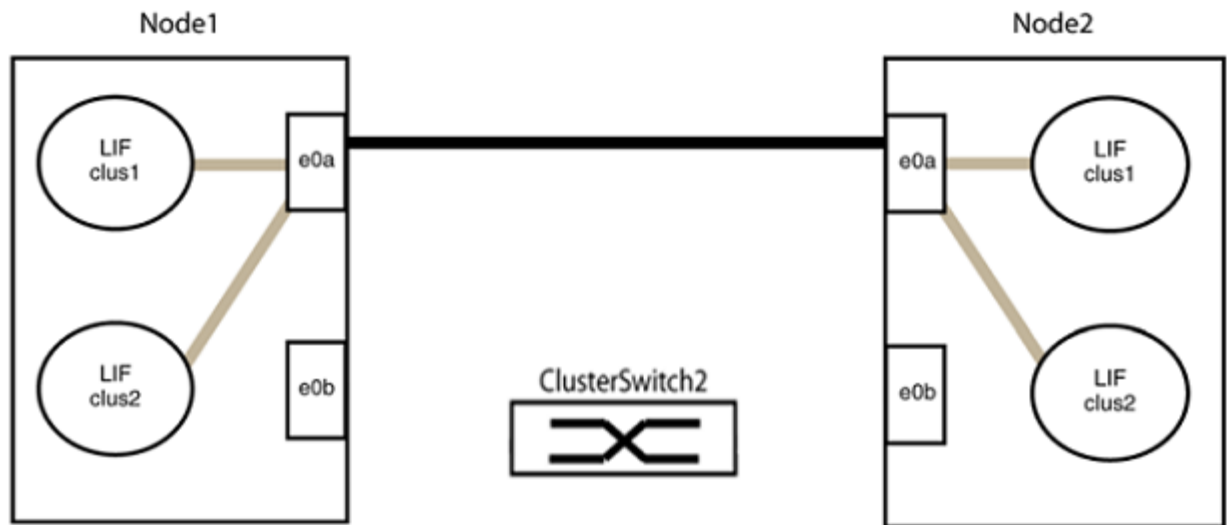
1. Configure la configuración sin switch para los puertos del grupo 2.



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**.

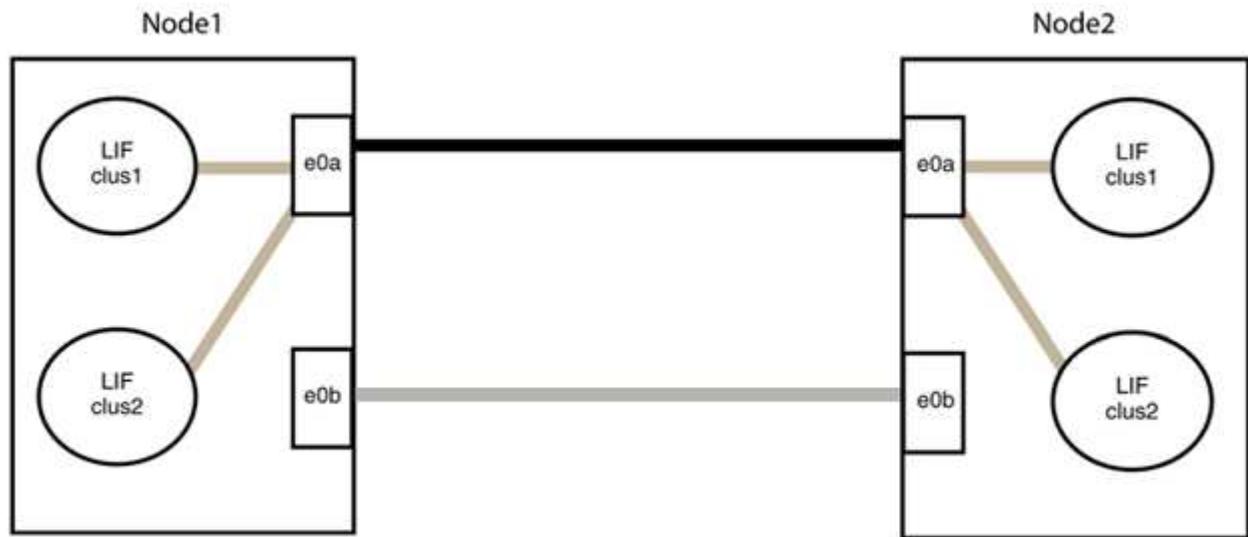
- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

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 épsilon en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

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

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

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

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

```

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

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

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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"](#).

2. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

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

Manos a la obra

Flujo de trabajo de instalación y configuración para los conmutadores de clúster Cisco Nexus 9336C-FX2 y 9336C-FX2-T

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

Los conmutadores de clúster le permiten crear clústeres ONTAP con más de dos nodos.

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

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

1

"Revisar los requisitos de configuración"

Revise los requisitos de configuración para los conmutadores de clúster 9336C-FX2 y 9336C-FX2-T.

2

"Revise los componentes y números de pieza"

Revise los componentes y números de pieza de los conmutadores de grupo 9336C-FX2 y 9336C-FX2-T.

3

"Revisar la documentación requerida"

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

4

"Revisar los requisitos de Smart Call Home"

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

5

"Instale el hardware"

Instale el hardware del interruptor.

6

"Configurar el software"

Configurar el software del conmutador.

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

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

Soporte de ONTAP

ONTAP 9.9.1 y versiones posteriores

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

Si desea crear clústeres de ONTAP con más de dos nodos, necesita dos switches de red compatibles.



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

ONTAP 9.10.1 y posteriores

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

Si desea crear clústeres de ONTAP con más de dos nodos, necesita dos switches de red compatibles.

Requisitos de configuración

Asegúrese de que:

- Tiene el número y tipo adecuados de cables y conectores de cable para los conmutadores. Consulte ["Hardware Universe"](#).
- Según el tipo de conmutador que esté configurando inicialmente, debe conectarse al puerto de la consola del conmutador con el cable de consola incluido.

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 AFF A700 de AFF, la interfaz e0M utiliza un puerto Ethernet dedicado.
- Consulte la ["Hardware Universe"](#) para obtener la información más reciente.

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

¿Qué sigue?

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

Componentes y números de pieza para Cisco switches de clúster Nexus 9336C-FX2 y 9336C-FX2-T.

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

Detalles del número de pieza

En la siguiente tabla, se enumeran el número de pieza y la descripción de los switches, los ventiladores y las fuentes de alimentación 9336C-FX2 y 9336C-FX2-T:

Número de pieza	Descripción
X190200-CS-PE	Switch de cluster, N9336C 36Pt PTSX 10/25/40/100g
X190200-CS-PI	Conmutador de grupo, N9336C 36Pt PSIN 10/25/40/100g
X190212-CS-PE	Switch de cluster, N9336C 12pt (9336C-FX2-T) PTSX 10/25/40/100g
X190212-CS-PI	Conmutador de grupo de instrumentos, N9336C 12pt (9336C-FX2-T) PSIN 10/25/40/100g
SW-N9K-FX2-24P-UPG	SW, Cisco 9336CFX2, licencia POD de 24 puertos
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40 GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100 GQSFP28
X190002	Kit de accesorios X190001/X190003
X-NXA-PAC-1100W-PE2	Fuente de alimentación de 1100 W ac N9K-9336C: Flujo de aire de escape lateral del puerto
X-NXA-PAC-1100W-PI2	Fuente de alimentación de 1100 W ac N9K-9336C - flujo de aire de entrada lateral del puerto
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, flujo de aire del lado de la lumbre
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, flujo de aire de entrada lateral de la lumbre

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

Para activar más de 12 puertos en su conmutador de clúster Cisco Nexus 9336C-FX-T, debe comprar una licencia inteligente de Cisco. Las licencias inteligentes de Cisco se administran a través de cuentas inteligentes de Cisco.

1. Cree una nueva cuenta Smart, si es necesario. Consulte ["Cree una nueva cuenta Smart"](#) para obtener más información.
2. Solicitar acceso a una cuenta Smart existente. Consulte ["Solicitar acceso a una cuenta Smart existente"](#) para obtener más información.



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

¿Qué sigue?

Después de haber confirmado sus componentes y números de pieza, revise el ["documentación requerida"](#) .

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

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

Documentación de los switches

Para configurar los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T, necesita la siguiente documentación del sitio web: ["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 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 9336-FX2 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 un switch Cisco 9336-FX2 en un armario de NetApp"	Describe cómo instalar los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T en un gabinete NetApp de cuatro postes.

Requisitos de Smart Call Home

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

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

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

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

- Debe haber un servidor de correo electrónico.
- 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

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

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

1

["Complete la hoja de trabajo 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.

2

["Instale el interruptor"](#)

Instale los interruptores 9336C-FX2 y 9336C-FX2-T.

3

["Instale el interruptor en un armario NetApp"](#)

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

4

["Revisar el cableado y la configuración"](#)

Revise el soporte para los puertos Ethernet de NVIDIA , los requisitos de FEC de 25 GbE y la información sobre los recursos de TCAM.

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

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 muestras 9336C-FX2](#)
- [Hoja de trabajo para el cableado en blanco 9336C-FX2](#)
- [Hoja de datos para el cableado de muestras 9336C-FX2-T \(12 puertos\)](#)

- [Hoja de datos para el cableado en blanco de 9336C-FX2-T \(12 puertos\)](#)

Hoja de trabajo para el cableado de muestras 9336C-FX2

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 de 10 GbE 1	1	4 nodos de 10 GbE 1
2	4 nodos de 10 GbE 2	2	4 nodos de 10 GbE 2
3	4 nodos 10 GbE 3	3	4 nodos 10 GbE 3
4	4 nodos de 25 GbE 4	4	4 nodos de 25 GbE 4
5	4 nodos de 25 GbE 5	5	4 nodos de 25 GbE 5
6	4 nodos de 25 GbE 6	6	4 nodos de 25 GbE 6
7	7 nodos 40/100GbE	7	7 nodos 40/100GbE
8	8 nodos 40/100GbE	8	8 nodos 40/100GbE
9	9 nodos 40/100GbE	9	9 nodos 40/100GbE
10	10 nodos 40/100GbE	10	10 nodos 40/100GbE
11	11 nodos 40/100GbE	11	11 nodos 40/100GbE
12	12 nodos 40/100GbE	12	12 nodos 40/100GbE
13	13 nodos 40/100GbE	13	13 nodos 40/100GbE
14	14 nodos 40/100GbE	14	14 nodos 40/100GbE
15	15 nodos 40/100GbE	15	15 nodos 40/100GbE
16	16 nodos 40/100GbE	16	16 nodos 40/100GbE
17	17 nodos 40/100GbE	17	17 nodos 40/100GbE
18	18 nodos 40/100GbE	18	18 nodos 40/100GbE
19	19 nodos 40/100GbE	19	19 nodos 40/100GbE

Switch de clúster a		Switch del clúster B	
20	20 nodos 40/100GbE	20	20 nodos 40/100GbE
21	21 nodos 40/100GbE	21	21 nodos 40/100GbE
22	22 nodos 40/100GbE	22	22 nodos 40/100GbE
23	23 nodos 40/100GbE	23	23 nodos 40/100GbE
24	24 nodos 40/100GbE	24	24 nodos 40/100GbE
25 hasta 34	Reservado	25 hasta 34	Reservado
35	100GbE ISL al puerto 35 del switch B	35	100GbE ISL para conmutar Un puerto 35
36	100GbE ISL al puerto 36 del switch B	36	100GbE ISL para conmutar Un puerto 36

Hoja de trabajo para el cableado en blanco 9336C-FX2

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	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	

Switch de clúster a		Switch del clúster B	
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 hasta 34	Reservado	25 hasta 34	Reservado
35	100GbE ISL al puerto 35 del switch B	35	100GbE ISL para conmutar Un puerto 35
36	100GbE ISL al puerto 36 del switch B	36	100GbE ISL para conmutar Un puerto 36

Hoja de datos para el cableado de muestras 9336C-FX2-T (12 puertos)

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

Switch de clúster a		Switch del clúster B	
1	4 nodos de 10 GbE 1	1	4 nodos de 10 GbE 1
2	4 nodos de 10 GbE 2	2	4 nodos de 10 GbE 2
3	4 nodos 10 GbE 3	3	4 nodos 10 GbE 3
4	4 nodos de 25 GbE 4	4	4 nodos de 25 GbE 4
5	4 nodos de 25 GbE 5	5	4 nodos de 25 GbE 5
6	4 nodos de 25 GbE 6	6	4 nodos de 25 GbE 6
7	7 nodos 40/100GbE	7	7 nodos 40/100GbE
8	8 nodos 40/100GbE	8	8 nodos 40/100GbE
9	9 nodos 40/100GbE	9	9 nodos 40/100GbE
10	10 nodos 40/100GbE	10	10 nodos 40/100GbE
11 hasta 34	Requiere licencia	11 hasta 34	Requiere licencia
35	100GbE ISL al puerto 35 del switch B	35	100GbE ISL para conmutar Un puerto 35
36	100GbE ISL al puerto 36 del switch B	36	100GbE ISL para conmutar Un puerto 36

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

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	
1		1	
2		2	
3		3	
4		4	

Switch de clúster a		Switch del clúster B	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11 hasta 34	Requiere licencia	11 hasta 34	Requiere licencia
35	100GbE ISL al puerto 35 del switch B	35	100GbE ISL para conmutar Un puerto 35
36	100GbE ISL al puerto 36 del switch B	36	100GbE ISL para conmutar Un puerto 36

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

¿Qué sigue?

Después de haber completado las hojas de trabajo de cableado, ["instalar el interruptor"](#) .

Instalar los conmutadores de clúster 9336C-FX2 y 9336C-FX2-T

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

Antes de empezar

Asegúrese de tener lo siguiente:

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones 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.
- Las licencias aplicables, la información de configuración y red, y los cables.
- Completado ["hojas de datos para el cableado"](#).
- Los RCF de red de gestión y red de clúster de NetApp aplicables descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#). 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.
- ["Documentación necesaria sobre el switch y ONTAP"](#).

Pasos

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

Si está instalando...	Realice lo siguiente...
Cisco Nexus 9336C-FX2 en un armario de sistemas de NetApp	Consulte la guía <i>instalación de un switch de clúster Cisco Nexus 9336C-FX2 y su panel de paso a través en un 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.

El futuro

Opcionalmente, puedes "[Instale un switch Cisco Nexus 9336C-FX2 en un armario de NetApp](#)". De lo contrario, vaya a "[revisar el cableado y la configuración](#)".

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

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

Antes de empezar

Asegúrese de tener lo siguiente:

- El kit de panel de paso a través, que está 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
- Para cada interruptor, ocho tornillos 10-32 ó 12-24 y tuercas de pinza para montar los soportes y rieles deslizantes en los postes del armario delantero y trasero.
- El kit de rieles estándar de Cisco para instalar el switch en un armario 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).

- Para conocer los requisitos iniciales de preparación, el contenido del kit y las precauciones de seguridad, consulte "[Guía de instalación de hardware de Cisco Nexus serie 9000](#)".

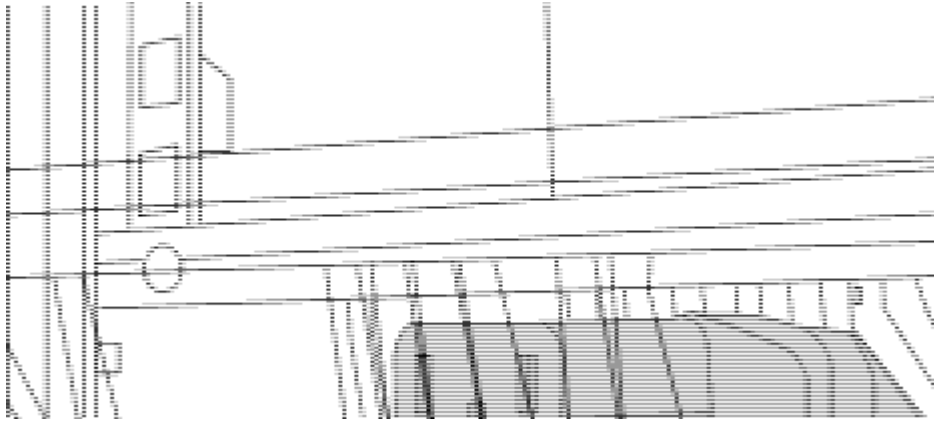
Pasos

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

- a. Determine la ubicación vertical de los interruptores y el panel de supresión en el armario.

En este procedimiento, el panel de limpieza se instala en U40.

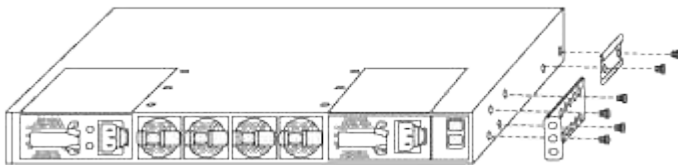
- b. Instale dos tuercas de abrazadera a cada lado en los orificios cuadrados adecuados para los rieles delanteros del armario.
- c. Centre el panel verticalmente para evitar intrusiones en el espacio adyacente del bastidor y, a continuación, apriete los tornillos.
- d. Inserte los conectores hembra de ambos cables puente de 48 pulgadas desde la parte posterior del panel y a través del conjunto del cepillo.



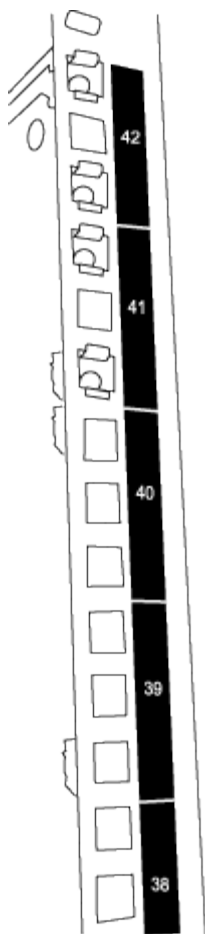
(1) conector hembra del cable puente.

2. Instale los soportes de montaje en rack en el chasis del switch Nexus 9336C-FX2.

- 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.



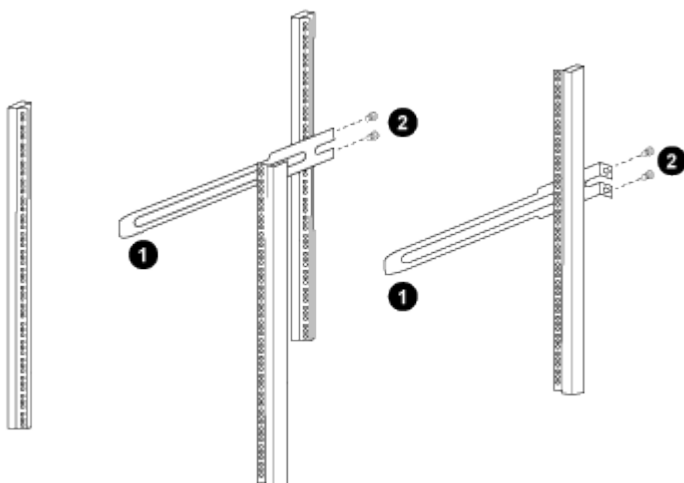
- b. Repita el paso 2a con el otro soporte de montaje en bastidor delantero en el otro lado del interruptor.
- c. Instale el soporte de montaje en bastidor trasero en el chasis del interruptor.
- d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del interruptor.
3. Instale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



Los dos conmutadores 9336C-FX2 y 9336C-FX2-T siempre se montan en la parte superior 2U del gabinete 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.

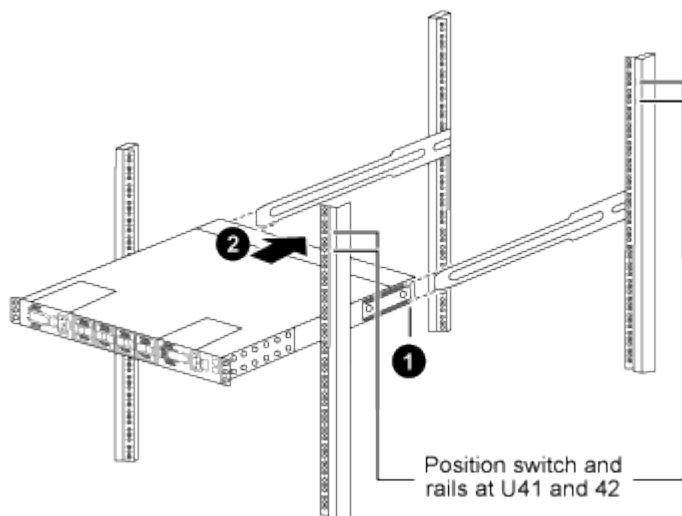
(2) apriete los tornillos de las guías deslizantes a los postes del armario.

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

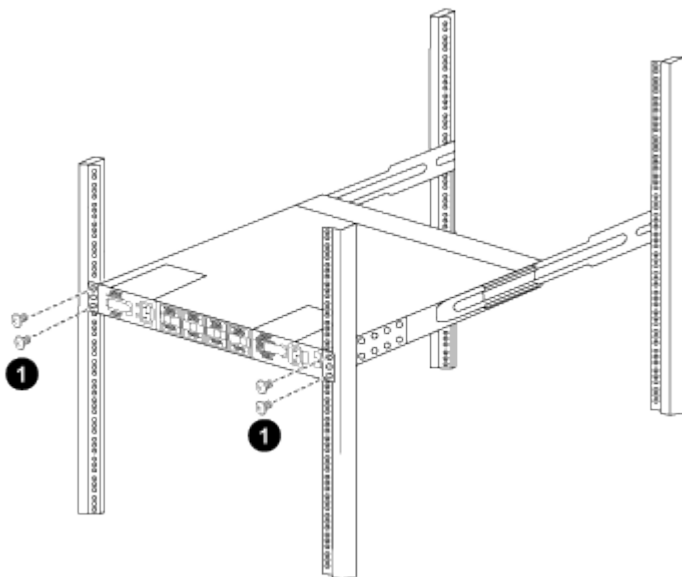
- a. Coloque la parte posterior del interruptor en RU41.



(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 delantera 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 conmutador 9336C-FX2 y 9336C-FX2-T a cualquiera de los conmutadores de administración (si se solicitaron) o conéctelos directamente a su 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.

El futuro

Después de haber instalado los conmutadores en el gabinete NetApp, "[configurar los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T](#)".

Revise las consideraciones sobre el cableado y la configuración

Antes de configurar los conmutadores 9336C-FX2 y 9336C-FX2-T, 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.

Puertos FAS2820 e0a/e0b

Los puertos e0a y e0b del FAS2820 requieren cambios de configuración de FEC para conectarse con los puertos de conmutador 9336C-FX2 y 9336C-FX2-T. Para los puertos de conmutación e0a y e0b, la configuración fec se establece en `rs-cons16`.

```
(cs1)(config)# interface Ethernet1/8-9
(cs1)(config-if-range)# fec rs-cons16
(cs1)(config-if-range)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Los puertos no se enlazan debido a los recursos de TCAM

En los conmutadores 9336C-FX2 y 9336C-FX2-T, los recursos de memoria direccionable por contenido ternario (TCAM) configurados en la configuración utilizada por el conmutador están agotados.

Consulte el artículo de la base de conocimientos ["Los puertos no se enlazan en Cisco Nexus 9336C-FX2 debido a recursos de TCAM"](#) para obtener información detallada sobre cómo resolver este problema.

Configurar el software

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

Para instalar y configurar el software de los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T e instalar o actualizar el archivo de configuración de referencia (RCF), siga estos pasos:

1

"Configure el switch"

Configurar los conmutadores de clúster 9336C-FX2 y 9336C-FX2-T.

2

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

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

3

"Instale o actualice el software NX-OS"

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

4

"Instale o actualice el RCF"

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

5

"Compruebe la configuración de SSH"

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

6

"Restablecer el interruptor a los valores predeterminados de fábrica"

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

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

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

Antes de empezar

Asegúrese de tener lo siguiente:

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones 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.
- Las licencias aplicables, la información de configuración y red, y los cables.
- Completado "hojas de datos para el cableado".
- Los RCF de red de gestión y red de clúster de NetApp aplicables descargados del sitio de soporte de NetApp en "mysupport.netapp.com". 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.
- "Documentación necesaria sobre el switch y ONTAP".

Pasos

1. 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.

Prompt	Respuesta
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.	Introduzca el nombre del switch, que 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
¿Habilitar el servicio telnet? (sí/no)	Responda con no . El valor predeterminado es no
¿Servicio SSH habilitado? (sí/no)	Responda con sí. El valor predeterminado es yes.  Se recomienda SSH cuando se utiliza Ethernet Switch Health Monitor (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.
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 a 2048.

Prompt	Respuesta
¿Configurar el servidor NTP? (sí/no)	Responda con no . El valor predeterminado es no
Configuración de 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)	Responda con sí para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.  Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador.

- 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

Después de haber configurado sus conmutadores, ["Prepárese para instalar el software NX-OS y RCF"](#) .

Prepárese para instalar el software NX-OS y RCF

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

Documentación sugerida

- ["Página del switch Cisco Ethernet"](#)

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

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

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

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

Proporciona información sobre actualizaciones o desactualizaciones disruptivas para el software Cisco NX-OS en los conmutadores Nexus serie 9000 en función de sus versiones actuales y futuras.

En la página, selecciona **Actualización disruptiva** y selecciona tu versión actual y la versión de destino de la lista desplegable.

Acerca de los ejemplos

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

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de nodo son cluster1-01 y cluster1-02.
- Los nombres de las LIF de 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 9000; 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	N9K-
C9336C	e0b	cs2	Eth1/2	N9K-
C9336C				
cluster1-01/cdp	e0a	cs1	Eth1/1	N9K-
C9336C	e0b	cs2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

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

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: cluster1-01
```

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
```

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					

node1					
	3/5/2022 19:21:18 -06:00		cluster1-01_clus2		cluster1-02-
clus1	none				
	3/5/2022 19:21:20 -06:00		cluster1-01_clus2		cluster1-
02_clus2	none				
node2					
	3/5/2022 19:21:18 -06:00		cluster1-02_clus2		cluster1-
01_clus1	none				
	3/5/2022 19:21:20 -06:00		cluster1-02_clus2		cluster1-
01_clus2	none				

Todos los lanzamientos de ONTAP

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

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



```

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

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

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

```

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

El futuro

Una vez que se haya preparado para instalar el software NX-OS y RCF, debe ["instalar o actualizar el software NX-OS"](#).

Instale o actualice el software NX-OS

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

Antes de comenzar, complete el procedimiento en ["Prepare la instalación de NX-OS y RCF"](#).

Revise los requisitos

Antes de empezar

Asegúrese de tener lo siguiente:

- 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

- ["Página del switch Cisco Ethernet"](#)

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

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

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

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

Proporciona información sobre actualización/degradación disruptiva para software Cisco NX-OS en los

switches de la serie Nexus 9000
en función de tus versiones actuales y objetivo.

En la página, selecciona **Actualización disruptiva** y selecciona tu versión actual y la versión de destino de la lista desplegable.

Acerca de los ejemplos

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

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

Instale el software

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.

Pasos

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el comando ping 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 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. 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      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C-FX2
cluster1::*>
```

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

a. Compruebe que todos los puertos del clúster están **up** con un 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
```

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

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

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

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

6. Copie las imágenes del software NX-OS y EPLD en el switch Nexus 9336C-FX2.

Muestra el ejemplo

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

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

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

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

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

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

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

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

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

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

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

8. Instale la imagen NX-OS.

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

Muestra el ejemplo

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

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

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

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

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

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

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

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

Compatibility check is done:

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

Images will be upgraded according to following table:

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

```
Switch will be reloaded for disruptive upgrade.
```

```
Do you want to continue with the installation (y/n)? [n] y
```

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

```
Performing runtime checks.
```

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

```
Setting boot variables.
```

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

```
Performing configuration copy.
```

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

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

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

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

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

9. 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 05.33
  NXOS: version 9.3(5)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.3.5.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

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

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

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

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

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

10. Actualice la imagen 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.9.3.5.img module all
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

11. Tras reiniciar el 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

12. 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 -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
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

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

cluster1-01/cdp	e0a	cs1	Ethernet1/7	N9K-
C9336C-FX2	e0d	cs2	Ethernet1/7	N9K-
C9336C-FX2				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C-FX2	e0d	cs2	Ethernet1/8	N9K-
C9336C-FX2				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/1	N9K-
C9336C-FX2				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/2	N9K-
C9336C-FX2				

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

Switch Model	Type	Address	

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

```

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

2 entries were displayed.

```

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.

```

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 6 a 13 para instalar el software NX-OS en el interruptor CS1.

15. Habilite la reversión automática en las LIF del clúster.

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

16. 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 LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

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

El futuro

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

Instale o actualice el RCF

Instale o actualice la descripción general del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar los

conmutadores Nexus 9336C-FX2 y 9336C-FX2-T por primera vez. Actualiza tu versión RCF cuando tienes una versión existente del archivo RCF instalado en tu conmutador.

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

Configuraciones de RCF disponibles

En la siguiente tabla se describen los CFR disponibles para diferentes configuraciones. Seleccione el RCF aplicable a su configuración.

Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

Nombre de RCF	Descripción
2-Cluster-HA-Breakout	Admite dos clústeres ONTAP con al menos ocho nodos, incluidos los nodos que utilizan puertos compartidos Cluster+HA.
4-Cluster-HA-Breakout	Admite cuatro clústeres ONTAP con al menos cuatro nodos, incluidos los nodos que utilizan puertos compartidos Cluster+HA.
1-Cluster-HA	Todos los puertos están configurados para 40/100GbE. Admite el tráfico de clúster/alta disponibilidad compartido en los puertos. Necesario para los sistemas AFF A320, AFF A250 y FAS500f. Además, todos los puertos se pueden utilizar como puertos de clúster dedicados.
1-Cluster-HA-Breakout	Los puertos se configuran para 4 puertos de separación de 10 GbE, 4 GbE (RCF 1,6+ en switches 100GbE) y 40/100GbE. Admite el tráfico compartido de clúster/alta disponibilidad en los puertos para los nodos que utilizan puertos de clúster/alta disponibilidad compartidos: Sistemas AFF A320, AFF A250 y FAS500f. Además, todos los puertos se pueden utilizar como puertos de clúster dedicados.
Cluster-HA-Storage	Los puertos se configuran para 40/100GbE para clúster+HA, 4 puertos separados de 10 GbE para clúster y 4 GbE para clúster+HA, y 100GbE para cada par de alta disponibilidad de almacenamiento.
Clúster	Dos variantes de RCF con diferentes asignaciones de 4 puertos 10 GbE (breakout) y de puertos 40/100GbE. Todos los nodos FAS/AFF son compatibles, excepto para los sistemas AFF A320, AFF A250 y FAS500f.
Reducida	Todos los puertos se configuran para conexiones de almacenamiento NVMe de 100GbE Gb.

Documentación sugerida

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

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

- ["Switches Cisco Nexus serie 3000"](#)

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

Acerca de los ejemplos

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

- Los nombres de los dos interruptores Cisco son **CS1** y **CS2**.
- Los nombres de los nodos son **cluster1-01**, **cluster1-02**, **cluster1-03** y **cluster1-04**.
- Los nombres de LIF de los clústeres son **cluster1-01_clus1**, **cluster1-04_clus2**, **cluster1-03_clus2**, **cluster1-03_clus1**, **cluster1-02_clus2**, **cluster1-02_clus1**, **cluster1-01_clus1** y **cluster1-04_clus1**.
- La `cluster1::*>` prompt indica el nombre del clúster.

En los ejemplos de este procedimiento se utilizan cuatro nodos. Estos nodos utilizan dos puertos de interconexión de clúster 10GbE **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.

Para obtener información detallada sobre las configuraciones de RCF disponibles, consulte ["Flujo de trabajo de instalación del software"](#).

Comandos utilizados

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.

El futuro

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

Instalación del archivo de configuración de referencia (RCF)

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

Antes de empezar

Compruebe las siguientes instalaciones y conexiones:

- Una conexión de consola al interruptor. La conexión de la consola es opcional si tiene acceso remoto al conmutador.
- El switch CS1 y el switch CS2 se encienden y la configuración inicial del switch se ha completado (la dirección IP de gestión y SSH está configurado).
- Se ha instalado la versión deseada de NX-OS.
- Las conexiones ISL entre los switches están conectadas.
- Los puertos del clúster de nodos de ONTAP no están conectados.

Paso 1: Instale el RCF en los interruptores

1. Inicie sesión en el switch CS1 mediante SSH o mediante una consola de serie.
2. Copie el RCF al bootflash del switch CS1 usando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP.

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

Muestra el ejemplo

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

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

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

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

En este ejemplo se muestra el archivo RCF Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt se está instalando en el interruptor cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
```

4. Examine el resultado del banner desde el `show banner motd` comando. Debe leer y seguir estas instrucciones para asegurarse de que la configuración y el funcionamiento del interruptor son correctos.

Muestra el ejemplo

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date       : 10-23-2020
* Version    : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

5. 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.

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

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

8. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.

Asegúrese de configurar lo siguiente:



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

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

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

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

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

9. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

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

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

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

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

10. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

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

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

```
cs1# write erase
```

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

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

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

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

13. Reinicie el interruptor CS1.

```
cs1# reload
```

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

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

15. Conecte los puertos de clúster de todos los nodos del clúster de ONTAP a los switches CS1 y CS2.

Paso 2: Verifique las conexiones del interruptor

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
show interface brief
```

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 los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes

comandos:

show vlan brief

show interface trunk

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/35, Eth1/36, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
17	VLAN0017	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
18	VLAN0018	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
31	VLAN0031	active	Eth1/11, Eth1/12, Eth1/13, Eth1/14, Eth1/15, Eth1/16, Eth1/17, Eth1/18, Eth1/19, Eth1/20, Eth1/21, Eth1/22
32	VLAN0032	active	Eth1/23, Eth1/24, Eth1/25

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
Eth1/34

```

```
cs1# show interface trunk
```

```

-----
Port                Native  Status      Port
                   Vlan                Channel
-----
Eth1/1              1      trunking    --
Eth1/2              1      trunking    --
Eth1/3              1      trunking    --
Eth1/4              1      trunking    --
Eth1/5              1      trunking    --
Eth1/6              1      trunking    --
Eth1/7              1      trunking    --
Eth1/8              1      trunking    --
Eth1/9/1            1      trunking    --
Eth1/9/2            1      trunking    --
Eth1/9/3            1      trunking    --
Eth1/9/4            1      trunking    --
Eth1/10/1           1      trunking    --
Eth1/10/2           1      trunking    --
Eth1/10/3           1      trunking    --
Eth1/10/4           1      trunking    --
Eth1/11             33     trunking    --

```


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

Port	Vlans Allowed on Trunk
Eth1/1	1,17-18
Eth1/2	1,17-18
Eth1/3	1,17-18
Eth1/4	1,17-18
Eth1/5	1,17-18
Eth1/6	1,17-18
Eth1/7	1,17-18
Eth1/8	1,17-18
Eth1/9/1	1,17-18
Eth1/9/2	1,17-18
Eth1/9/3	1,17-18
Eth1/9/4	1,17-18
Eth1/10/1	1,17-18
Eth1/10/2	1,17-18
Eth1/10/3	1,17-18
Eth1/10/4	1,17-18

```

Eth1/11      31,33
Eth1/12      31,33
Eth1/13      31,33
Eth1/14      31,33
Eth1/15      31,33
Eth1/16      31,33
Eth1/17      31,33
Eth1/18      31,33
Eth1/19      31,33
Eth1/20      31,33
Eth1/21      31,33
Eth1/22      31,33
Eth1/23      32,34
Eth1/24      32,34
Eth1/25      32,34
Eth1/26      32,34
Eth1/27      32,34
Eth1/28      32,34
Eth1/29      32,34
Eth1/30      32,34
Eth1/31      32,34
Eth1/32      32,34
Eth1/33      32,34
Eth1/34      32,34
Eth1/35      1
Eth1/36      1
Po1          1
..
..
..
..
..

```



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

3. 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      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

Paso 3: Configure el cluster ONTAP

NetApp recomienda usar System Manager para configurar clústeres nuevos.

System Manager proporciona un flujo de trabajo sencillo y sencillo para la instalación y la configuración del clúster, incluidas la asignación de una dirección IP de gestión de nodos, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento del almacenamiento inicial.

Vaya a ["Configure ONTAP en un nuevo clúster con System Manager"](#) para obtener instrucciones de configuración.

El futuro

Después de haber instalado el RCF, ["verificar la configuración de SSH"](#) .

Actualice su archivo de configuración de referencia (RCF)

Actualice la versión de RCF cuando tenga instalada una versión existente del archivo RCF en los conmutadores operativos.

Antes de empezar

Asegúrese de tener lo siguiente:

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

Si necesita cambiar la configuración 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.



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.



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

Paso 1: Prepárese para la actualización

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      N9K-
C9336C
          e0d    cs2                Ethernet1/7      N9K-
C9336C
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C
          e0d    cs2                Ethernet1/8      N9K-
C9336C
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C
cluster1::*>
```

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

a. Compruebe que todos los puertos del clúster están **up** con un 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
```

	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			
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                                     Type                                     Address  
Model  
-----  
-----  
cs1                                     cluster-network                       10.233.205.90      N9K-  
C9336C  
    Serial Number: FOCXXXXXXGD  
    Is Monitored: true  
    Reason: None  
    Software Version: Cisco Nexus Operating System (NX-OS) Software,  
Version  
                        9.3(5)  
    Version Source: CDP  
  
cs2                                     cluster-network                       10.233.205.91      N9K-  
C9336C  
    Serial Number: FOCXXXXXXGS  
    Is Monitored: true  
    Reason: None  
    Software Version: Cisco Nexus Operating System (NX-OS) Software,  
Version  
                        9.3(5)  
    Version Source: CDP  
cluster1::*>
```

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

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

Paso 2: Configurar puertos

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

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

```
cs1(config-if-range)# exit
```

```
cs1# exit
```



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

2. Compruebe que las LIF del clúster han conmutado al nodo de respaldo a los puertos alojados en el switch del clúster CS1. 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::*>
```

3. 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::*>
```

4. 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
```

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



Asegúrese de configurar lo siguiente:

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

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

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

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

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

6. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

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

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

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

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

7. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

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

8. Ejecute el comando `WRITE BORRATE` para borrar la configuración guardada actual:

```
cs1# write erase
```

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

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

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

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

10. Reinicie el conmutador:

```
switch# reload
```

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

11. Cuando se pueda volver a acceder a la dirección IP de administración, inicie sesión en el switch a través de SSH.

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

12. Copie el RCF al bootflash del switch CS1 usando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP.

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

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_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)...
```

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

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

En este ejemplo se muestra el archivo RCF `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` se está instalando en el interruptor `cs1`:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-config
echo-commands
```



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

14. 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.

15. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.
16. Después de comprobar que las versiones de RCF, las adiciones personalizadas y la configuración del switch son correctas, copie el archivo `running-config` en el archivo `startup-config`.

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

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

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

17. Reinicie el interruptor `CS1`. Puede ignorar las alertas de «monitor de estado del switch del clúster» y los eventos de «puertos inactivos» que se notifican en los nodos mientras se reinicia el switch.

```
cs1# reload
```

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

18. 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 -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
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-01/cdp	e0a	cs1	Ethernet1/7	N9K-
C9336C	e0d	cs2	Ethernet1/7	N9K-
C9336C				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C	e0d	cs2	Ethernet1/8	N9K-
C9336C				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N9K-
C9336C	e0b	cs2	Ethernet1/1/1	N9K-
C9336C				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N9K-
C9336C	e0b	cs2	Ethernet1/1/2	N9K-
C9336C				

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

Switch Model	Type	Address	
cs1	cluster-network	10.233.205.90	NX9-
C9336C			
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	NX9-


```

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

2 entries were displayed.

```

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.

```

19. 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::*>

```

20. Repita los pasos 1 a 19 en el interruptor cs2.

21. Habilite la reversión automática en las LIF del clúster.

```

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

```

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

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
show interface brief
```

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 los nodos esperados siguen conectados:

```
show cdp neighbors
```

Muestra el ejemplo

```
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
cs1 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

Total entries displayed: 4

3. Compruebe que los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Po1, Eth1/1, Eth1/2, Eth1/3 Eth1/4, Eth1/5, Eth1/6, Eth1/7 Eth1/8, Eth1/35, Eth1/36 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
17	VLAN0017	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
18	VLAN0018	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
31	VLAN0031	active	Eth1/11, Eth1/12, Eth1/13 Eth1/14, Eth1/15, Eth1/16 Eth1/17, Eth1/18, Eth1/19 Eth1/20, Eth1/21, Eth1/22
32	VLAN0032	active	Eth1/23, Eth1/24, Eth1/25

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active
Eth1/25
Eth1/28
Eth1/31
Eth1/34
Eth1/26, Eth1/27,
Eth1/29, Eth1/30,
Eth1/32, Eth1/33,
Eth1/11, Eth1/12,
Eth1/14, Eth1/15,
Eth1/17, Eth1/18,
Eth1/20, Eth1/21,
Eth1/23, Eth1/24,
Eth1/26, Eth1/27,
Eth1/29, Eth1/30,
Eth1/32, Eth1/33,

```

```
cs1# show interface trunk
```

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--
Eth1/9/1	1	trunking	--
Eth1/9/2	1	trunking	--
Eth1/9/3	1	trunking	--
Eth1/9/4	1	trunking	--
Eth1/10/1	1	trunking	--
Eth1/10/2	1	trunking	--
Eth1/10/3	1	trunking	--
Eth1/10/4	1	trunking	--
Eth1/11	33	trunking	--

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

```

-----
Port                Vlans Allowed on Trunk
-----
Eth1/1              1,17-18
Eth1/2              1,17-18
Eth1/3              1,17-18
Eth1/4              1,17-18
Eth1/5              1,17-18
Eth1/6              1,17-18
Eth1/7              1,17-18
Eth1/8              1,17-18
Eth1/9/1            1,17-18
Eth1/9/2            1,17-18
Eth1/9/3            1,17-18
Eth1/9/4            1,17-18
Eth1/10/1           1,17-18
Eth1/10/2           1,17-18
Eth1/10/3           1,17-18
Eth1/10/4           1,17-18

```

```
Eth1/11      31,33
Eth1/12      31,33
Eth1/13      31,33
Eth1/14      31,33
Eth1/15      31,33
Eth1/16      31,33
Eth1/17      31,33
Eth1/18      31,33
Eth1/19      31,33
Eth1/20      31,33
Eth1/21      31,33
Eth1/22      31,33
Eth1/23      32,34
Eth1/24      32,34
Eth1/25      32,34
Eth1/26      32,34
Eth1/27      32,34
Eth1/28      32,34
Eth1/29      32,34
Eth1/30      32,34
Eth1/31      32,34
Eth1/32      32,34
Eth1/33      32,34
Eth1/34      32,34
Eth1/35      1
Eth1/36      1
Po1          1
..
..
..
..
..
```



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

4. 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      Pol (SU)      Eth      LACP      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

5. 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 LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

```
network interface revert -vserver vservice_name -lif lif_name
```

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

Packet	Source	Destination
Node	Date	LIF
Loss		

node1		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-
clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-
02_clus2 none		
node2		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-
01_clus1 none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-
01_clus2 none		

Todos los lanzamientos de ONTAP

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

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

```

cluster1::~*> cluster ping-cluster -node local
Host is 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)

```

El futuro

Después de haber actualizado su RCF, ["verificar la configuración de SSH"](#) .

Compruebe su configuración SSH

Si utiliza la supervisión de estado del switch Ethernet (CSHM) y las funciones de

recogida de registros, compruebe que las claves SSH y SSH estén habilitadas en los switches de clústeres.

Pasos

1. Compruebe que SSH está habilitado:

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

2. Compruebe que las claves SSH estén habilitadas:

```
show ssh key
```

Muestra el ejemplo

```
(switch)# show ssh key

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

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yIPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDsrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

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



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

El futuro

Después de haber verificado su configuración SSH, ["configurar la monitorización del estado del conmutador"](#).

Restablecer los interruptores de clúster 9336C-FX2 y 9336C-FX2-T a los valores predeterminados de fábrica

Para restablecer los interruptores del clúster 9336C-FX2 y 9336C-FX2-T a los valores predeterminados de fábrica, debe borrar la configuración de los interruptores 9336C-FX2 y 9336C-FX2-T.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Borrar la configuración existente:

```
write erase
```

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

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

2. Recargue el software del conmutador:

```
reload
```

```
(cs2)# reload
```

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

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

Migrar los switches

Migrar de los conmutadores de clúster NetApp CN1610 a los conmutadores de clúster Cisco 9336C-FX2 y 9336C-FX2-T

Puede migrar conmutadores de clúster CN1610 de NetApp para un clúster ONTAP a conmutadores de clúster Cisco 9336C-FX2 y 9336C-FX2-T. Este es un procedimiento que no produce interrupciones.

Revise los requisitos

Debe tener en cuenta cierta información de configuración, conexiones de puertos y requisitos de cableado cuando reemplace los conmutadores de clúster NetApp CN1610 con conmutadores de clúster Cisco 9336C-FX2 y 9336C-FX2-T. También debe verificar el número de serie del conmutador para asegurarse de que se

migre el conmutador correcto.

Switches compatibles

Se admiten los siguientes switches de clúster:

- CN1610 de NetApp
- Cisco 9336C-FX2
- Cisco 9336C-FX2-T

Para obtener más información acerca de los puertos admitidos y sus configuraciones, consulte "[Hardware Universe](#)".

Lo que necesitará

Compruebe que la configuración cumple los siguientes requisitos:

- El clúster existente está correctamente configurado y funcionando.
- Todos los puertos de clúster se encuentran en el estado **up** para garantizar operaciones no disruptivas.
- Los conmutadores de clúster Cisco 9336C-FX2 y 9336C-FX2-T están configurados y funcionando con la versión correcta de NX-OS instalada con el archivo de configuración de referencia (RCF) aplicado.
- La configuración de red del clúster existente tiene lo siguiente:
 - Un clúster de NetApp redundante y completamente funcional mediante switches NetApp CN1610.
 - Conectividad de gestión y acceso mediante consola a los switches NetApp CN1610 y a los nuevos.
 - Todos los LIF del clúster con las LIF del clúster están en sus puertos de inicio.
- Algunos de los puertos están configurados en los conmutadores Cisco 9336C-FX2 y 9336C-FX2-T para funcionar a 40 GbE o 100 GbE.
- Ha planificado, migrado y documentado la conectividad de 40 GbE y 100 GbE desde los nodos a los conmutadores de clúster Cisco 9336C-FX2 y 9336C-FX2-T.

Migrar los switches

Acerca de los ejemplos

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

- Los switches de clúster CN1610 existentes son *C1* y *C2*.
- Los nuevos switches de clúster 9336C-FX2 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.
- La `cluster1::*>` prompt indica el nombre del clúster.
- Los puertos de clúster utilizados en este procedimiento son *e3a* y *e3b*.

Acerca de esta tarea

Este procedimiento cubre el siguiente caso:

- El interruptor C2 se reemplaza primero por el interruptor CS2.
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.

- Todos los LIF de clúster conmutan al nuevo switch CS2.
- Después, el cableado entre los nodos y C2 se desconecta del C2 y se vuelve a conectar al CS2.
- El interruptor C1 se reemplaza por el interruptor CS1.
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - Todos los LIF de clúster conmutan al nuevo switch CS1.
 - Después, el cableado entre los nodos y C1 se desconecta del C1 y se vuelve a conectar al CS1.



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 conmuta por error todos los LIF de clúster al switch operativo asociado mientras realiza los pasos en el switch de destino.

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
```

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

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

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

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

Al deshabilitar la reversión automática para este procedimiento, los LIF del clúster no volverán a moverse automáticamente a su puerto principal. Permanecen en el puerto actual mientras continúa funcionando.

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

Paso 2: Configure los puertos y el cableado

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

Cada puerto debería mostrarse para Link y.. healthy 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
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
-----	-----				
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

b. Muestre información sobre las LIF y sus nodos iniciales designados:

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

Cada LIF debería mostrar up/up para Status Admin/Oper y.. true 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					
e3a		node1_clus1	up/up	169.254.209.69/16	node1
	true	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true				
e3a		node2_clus1	up/up	169.254.47.194/16	node2
	true	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true				

2. Los puertos de 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
```

Muestra el ejemplo

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

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

node1	/cdp			
	e3a	C1	(6a:ad:4f:98:3b:3f)	0/1 -
	e3b	C2	(6a:ad:4f:98:4c:a4)	0/1 -
node2	/cdp			
	e3a	C1	(6a:ad:4f:98:3b:3f)	0/2 -
	e3b	C2	(6a:ad:4f:98:4c:a4)	0/2 -

3. Los puertos y los switches del clúster se conectan 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 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
C2 0/13	0/13	179	S I s	CN1610
C2 0/14	0/14	175	S I s	CN1610
C2 0/15	0/15	179	S I s	CN1610
C2 0/16	0/16	175	S I s	CN1610

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 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
C1 0/13	0/13	175	S I s	CN1610
C1 0/14	0/14	175	S I s	CN1610
C1 0/15	0/15	175	S I s	CN1610
C1 0/16	0/16	175	S I s	CN1610

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

ONTAP 9.9.1 y versiones posteriores

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

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

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

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

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

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

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

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e3a
Cluster node1_clus2 169.254.49.125 node1      e3b
Cluster node2_clus1 169.254.47.194 node2      e3a
Cluster node2_clus2 169.254.19.183 node2      e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. En el switch C2, apague los puertos conectados a los puertos de cluster de los nodos para conmutar las LIF de cluster.



No intente migrar manualmente las LIF de clúster.

```

(C2)# configure
(C2)(Config)# interface 0/1-0/12
(C2)(Interface 0/1-0/12)# shutdown
(C2)(Interface 0/1-0/12)# exit
(C2)(Config)# exit

```

2. Mueva los puertos del clúster de nodos del antiguo conmutador C2 al nuevo conmutador cs2, utilizando el cableado adecuado compatible con Cisco 9336C-FX2 y 9336C-FX2-T.
3. Mostrar los atributos del puerto de red:

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


Muestra el ejemplo

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

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

4. 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
```

Muestra el ejemplo

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node1	/cdp			
	e3a	C1 (6a:ad:4f:98:3b:3f)	0/1	
CN1610				
	e3b	cs2 (b8:ce:f6:19:1a:7e)	Ethernet1/1/1	N9K-
C9336C-FX2				
node2	/cdp			
	e3a	C1 (6a:ad:4f:98:3b:3f)	0/2	
CN1610				
	e3b	cs2 (b8:ce:f6:19:1b:96)	Ethernet1/1/2	N9K-
C9336C-FX2				

5. En el switch CS2, compruebe que todos los puertos de clúster de nodos estén activos:

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

Muestra el ejemplo

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

Current Is	Logical	Status	Network	Current
Vserver	Interfac	Admin/Oper	Address/Mask	Node
Port	Home			
Cluster				
	node1_clus1	up/up	169.254.3.4/16	node1
e0b	false			
	node1_clus2	up/up	169.254.3.5/16	node1
e0b	true			
	node2_clus1	up/up	169.254.3.8/16	node2
e0b	false			
	node2_clus2	up/up	169.254.3.9/16	node2
e0b	true			

6. En el switch C1, apague los puertos conectados a los puertos de clúster de los nodos para conmutar las LIF de clúster.

```
(C1) # configure
(C1) (Config) # interface 0/1-0/12
(C1) (Interface 0/1-0/12) # shutdown
(C1) (Interface 0/1-0/12) # exit
(C1) (Config) # exit
```

7. Mueva los puertos del clúster de nodos del antiguo conmutador C1 al nuevo conmutador cs1, utilizando el cableado adecuado compatible con Cisco 9336C-FX2 y 9336C-FX2-T.
8. Compruebe la configuración final del clúster:

```
network port show -ipSPACE Cluster
```

Cada puerto debe aparecer up para Link y.. healthy 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							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

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
```

Muestra el ejemplo

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node1	/cdp			
	e3a	cs1 (b8:ce:f6:19:1a:7e)	Ethernet1/1/1	N9K-
C9336C-FX2				
	e3b	cs2 (b8:ce:f6:19:1b:96)	Ethernet1/1/2	N9K-
C9336C-FX2				
node2	/cdp			
	e3a	cs1 (b8:ce:f6:19:1a:7e)	Ethernet1/1/1	N9K-
C9336C-FX2				
	e3b	cs2 (b8:ce:f6:19:1b:96)	Ethernet1/1/2	N9K-
C9336C-FX2				

10. En los switches CS1 y CS2, compruebe que todos los puertos del clúster de nodos estén activos:

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

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

11. Compruebe que ambos nodos tengan una conexión cada uno con cada switch:

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

Muestra el ejemplo

En el siguiente ejemplo, se muestran los resultados adecuados para ambos switches:

```
cluster1::*> network device-discovery show -protocol cdp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1         /cdp
              e0a    cs1 (b8:ce:f6:19:1b:42)  Ethernet1/1/1  N9K-
C9336C-FX2
              e0b    cs2 (b8:ce:f6:19:1b:96)  Ethernet1/1/2  N9K-
C9336C-FX2
node2         /cdp
              e0a    cs1 (b8:ce:f6:19:1b:42)  Ethernet1/1/1  N9K-
C9336C-FX2
              e0b    cs2 (b8:ce:f6:19:1b:96)  Ethernet1/1/2  N9K-
C9336C-FX2
```

Paso 3: Verificar la configuración

1. Habilite la reversión automática en las LIF del clúster:

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

2. Compruebe que todos los LIF de red del clúster vuelven a estar en sus puertos raíz:

```
network interface show
```

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				
e3a	node1_clus1	up/up	169.254.209.69/16	node1
e3b	true			
e3a	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true			
e3a	node2_clus1	up/up	169.254.47.194/16	node2
e3b	true			
e3a	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true			

3. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

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
```

El futuro

Después de haber migrado sus conmutadores, ["configurar la monitorización del estado del conmutador"](#) .

Migrar de conmutadores Cisco más antiguos a conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Puede realizar una migración sin interrupciones desde conmutadores de clúster Cisco más antiguos a conmutadores de red de clúster Cisco Nexus 9336C-FX2 y 9336C-FX2-T.

Revise los requisitos

Asegúrese de que:

- Ha verificado el número de serie del conmutador para asegurarse de que se migra el conmutador correcto.
- Algunos de los puertos de los switches Nexus 9336C-FX2 están configurados para funcionar a 10GbE o 40GbE GbE.
- Se ha planificado, migrado y documentado la conectividad 10GbE y 40GbE desde los nodos a los

switches del clúster Nexus 9336C-FX2.

- El clúster está funcionando completamente (no debería haber errores en los registros o problemas similares).
- La personalización inicial de los switches Cisco Nexus 9336C-FX2 finaliza para que:
 - Los switches 9336C-FX2 ejecutan la versión de software recomendada más reciente.
 - Confirme que los archivos de configuración de referencia (RFC) se han aplicado por completo a cualquier switch nuevo antes de migrar las LIF a los nuevos switches.
 - Compruebe las configuraciones de funcionamiento e inicio en ambos switches antes de cambiar el tráfico de red.
 - La personalización de cualquier sitio, como DNS, NTP, SMTP, SNMP, Y SSH, se configuran en los nuevos switches.
- Tiene acceso a la tabla de compatibilidad del conmutador de ["Switches Ethernet de Cisco"](#) Para las versiones ONTAP, NX-OS y RCF admitidas.
- Ha revisado las guías de actualización y software adecuadas disponibles en el sitio web de Cisco para los procedimientos de actualización y degradación de switches de Cisco en ["Compatibilidad con los switches Cisco Nexus serie 9000"](#) página.



Si está cambiando la velocidad de puerto de los puertos de los clústeres de e0a y e1a en sistemas AFF A800 o AFF C800, puede observar que se están recibiendo paquetes con formato incorrecto tras la conversión de velocidad. Consulte ["Error 1570339"](#) Y el artículo de la base de conocimientos ["Errores de CRC en puertos T6 después de convertir de 40GbE a 100GbE"](#) para obtener orientación.

Migrar los switches

Acerca de los ejemplos

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

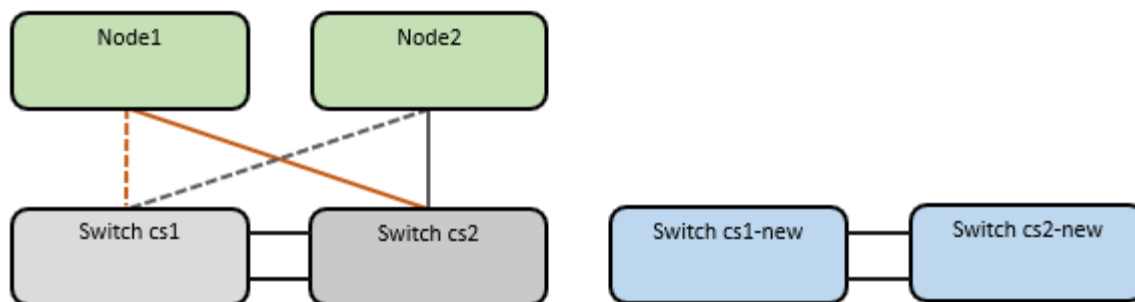


Los resultados del comando pueden variar en función de las diferentes versiones de ONTAP.

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

- Los nombres de los dos conmutadores Cisco existentes son **cs1** y **cs2**
- Los nuevos switches de clúster Nexus 9336C-FX2 son **cs1-new** y **cs2-new**.
- Los nombres de los nodos son **1** y **2**.
- Los nombres de LIF del clúster son **1_clus1** y **1_clus2** para el nodo 1, y **2_clus1** y **2_clus2** para el nodo 2.
- El símbolo **cluster1:>*** indica el nombre del clúster.

Durante este procedimiento, consulte el siguiente ejemplo:



Acerca de esta tarea

El procedimiento requiere el uso de tanto comandos de la ONTAP como de ["Switches de la serie Nexus 9000"](#) Comandos; los comandos de ONTAP se utilizan, a menos que se indique lo contrario.

Este procedimiento cubre el siguiente caso:

- El interruptor CS2 se reemplaza por el interruptor CS2-NUEVO primero.
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - Todos los LIF de clúster conmutan al nuevo switch CS2-new.
 - Después, el cableado entre los nodos y CS2 se desconecta del CS2 y se vuelve a conectar a CS2 nuevo.
- El interruptor CS1 se reemplaza por el interruptor CS1-NUEVO.
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - Todos los LIF de clúster conmutan al nuevo switch CS1-new.
 - Después, el cableado entre los nodos y CS1 se desconecta del CS1 y se vuelve a conectar a CS1 nuevo.



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 conmuta por error todos los LIF de clúster al switch operativo asociado mientras realiza los pasos en el switch de destino.

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` 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
```

Aparece el mensaje avanzado (*>).

Paso 2: Configure los puertos y el cableado

1. En los switches nuevos, confirme que el ISL se ha cableado y está en buen estado entre los switches cs1-new y cs2-new:

```
show port-channel summary
```

Muestra el ejemplo

```
cs1-new# 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      Eth1/35(P)  Eth1/36(P)

cs2-new# 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      Eth1/35(P)  Eth1/36(P)
```

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

```
network device-discovery show
```

Muestra el ejemplo

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

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

node1	/cdp		
	e0a	cs1	Ethernet1/1 N5K-
C5596UP			
	e0b	cs2	Ethernet1/2 N5K-
C5596UP			
node2	/cdp		
	e0a	cs1	Ethernet1/1 N5K-
C5596UP			
	e0b	cs2	Ethernet1/2 N5K-
C5596UP			

3. Determinar el estado administrativo u operativo de cada puerto de 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
Status	Status				Admin/Oper
-----	-----	-----	----	----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e0b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node2

Ignore

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

- b. Compruebe que todas las interfaces del clúster (LIF) están en sus puertos de inicio:

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

Muestra el ejemplo

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

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

Cluster					
e0a	true	node1_clus1	up/up	169.254.209.69/16	node1
e0b	true	node1_clus2	up/up	169.254.49.125/16	node1
e0a	true	node2_clus1	up/up	169.254.47.194/16	node2
e0b	true	node2_clus2	up/up	169.254.19.183/16	node2

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 C5596UP	cluster-network	10.233.205.92	N5K-
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 C5596UP	cluster-network	10.233.205.93	N5K-
Serial Number: FOXXXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(4)			
Version Source: CDP			

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

Al deshabilitar la reversión automática para este procedimiento, los LIF del clúster no volverán a moverse automáticamente a su puerto principal. Permanecen en el puerto actual mientras continúa funcionando.

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



Al deshabilitar la reversión automática se garantiza que ONTAP solo conmute a través de los LIF del clúster cuando los puertos del switch se apagen más adelante.

5. En el conmutador de clúster CS2, apague los puertos conectados a los puertos de clúster de **todos** los nodos para conmutar por error las LIF de clúster:


```

cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2(config)# exit
cs2#

```

6. Compruebe que las LIF del clúster han conmutado al nodo de respaldo a los puertos alojados en el switch del clúster CS1. 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	169.254.3.4/16	node1
e0a	true			
	node1_clus2	up/up	169.254.3.5/16	node1
e0a	false			
	node2_clus1	up/up	169.254.3.8/16	node2
e0a	true			
	node2_clus2	up/up	169.254.3.9/16	node2
e0a	false			

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

8. Si las LIF de clúster han conmutado al switch CS1 y el estado del clúster es bueno, vaya a [Paso. 10](#). Si algunos LIF del clúster no están en buen estado o el clúster está en mal estado, puede revertir la conectividad al switch CS2 de la siguiente manera:

- a. Abra los puertos conectados a los puertos del cluster de **all** los nodos:

```
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# no shutdown
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

- b. Compruebe que las LIF del clúster han conmutado al nodo de respaldo a los puertos alojados en el switch del clúster CS1. 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	169.254.3.4/16	node1
e0a	true			
	node1_clus2	up/up	169.254.3.5/16	node1
e0a	false			
	node2_clus1	up/up	169.254.3.8/16	node2
e0a	true			
	node2_clus2	up/up	169.254.3.9/16	node2
e0a	false			

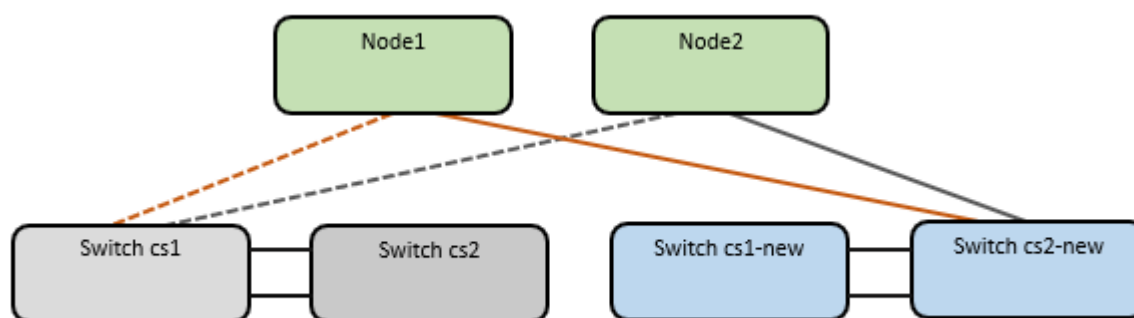
- c. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

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

9. Una vez que haya restaurado el estado de LIF y del clúster, reinicie el proceso desde [Paso. 4](#).
10. Mueva todos los cables de conexión de nodo de clúster del antiguo conmutador CS2 al nuevo conmutador CS2-new.
 - Cables de conexión de nodo de clúster movidos al switch CS2-new*



11. Confirme el estado de las conexiones de red movidas a cs2-new:

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

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

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

Todos los puertos del clúster que se movieron deben estar en funcionamiento.

12. Compruebe la información de cercanía en los puertos de clúster:

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

Muestra el ejemplo

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

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

node1	/cdp			
	e0a	cs1	Ethernet1/1	N5K-
C5596UP				
	e0b	cs2-new	Ethernet1/1/1	N9K-
C9336C-FX2				
node2	/cdp			
	e0a	cs1	Ethernet1/2	N5K-
C5596UP				
	e0b	cs2-new	Ethernet1/1/2	N9K-
C9336C-FX2				

Compruebe que los puertos del clúster movidos ven al conmutador cs2-new como vecino.

13. Confirme las conexiones de puertos del switch desde la perspectiva del switch CS2-new:

```
cs2-new# show interface brief
cs2-new# show cdp neighbors
```

14. En el conmutador de clúster CS1, apague los puertos conectados a los puertos de clúster de **todos** los nodos para conmutar por error las LIF de clúster.

```
cs1# configure
cs1(config)# interface eth1/1-1/2
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit
cs1#
```

Todos los LIF del clúster conmutan al nodo de respaldo en el switch CS2 nuevo.

15. Compruebe que los LIF del clúster han conmutado al nodo de respaldo en los puertos alojados en el switch CS2-new. Esto puede tardar unos segundos:

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

Muestra el ejemplo

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

Current Is	Logical	Status	Network	Current
Vserver	Interfac	Admin/Oper	Address/Mask	Node
Port	Home			
Cluster				
e0b	node1_clus1	up/up	169.254.3.4/16	node1
e0b	node1_clus2	up/up	169.254.3.5/16	node1
e0b	node2_clus1	up/up	169.254.3.8/16	node2
e0b	node2_clus2	up/up	169.254.3.9/16	node2

16. Compruebe que el clúster esté en buen estado:

```
cluster show
```

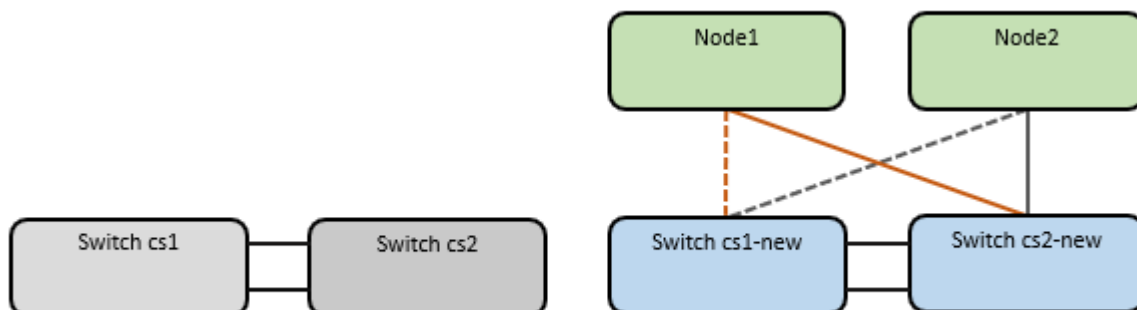
Muestra el ejemplo

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1	true	true	false
node2	true	true	false

17. Mueva los cables de conexión de nodo de clúster de CS1 al nuevo switch de CS1 nuevos.

- Cables de conexión de nodo de clúster movidos al switch CS1-new*



18. Confirme el estado de las conexiones de red movidas a cs1-new:

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

Muestra el ejemplo

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

Node: node1

Ignore

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

Node: node2

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
e0a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

Todos los puertos del clúster que se movieron deben estar en funcionamiento.

19. Compruebe la información de cercanía en los puertos de clúster:

```
network device-discovery show
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

node1	/cdp			
	e0a	cs1-new	Ethernet1/1/1	N9K-
C9336C-FX2				
	e0b	cs2-new	Ethernet1/1/2	N9K-
C9336C-FX2				
node2	/cdp			
	e0a	cs1-new	Ethernet1/1/1	N9K-
C9336C-FX2				
	e0b	cs2-new	Ethernet1/1/2	N9K-
C9336C-FX2				

Compruebe que los puertos del clúster movidos ven al switch cs1-new como vecino.

20. Confirme las conexiones de puertos del switch desde la perspectiva del switch CS1-new:

```
cs1-new# show interface brief
cs1-new# show cdp neighbors
```

21. Compruebe que el ISL entre cs1-new y cs2-new siga operativo:

```
show port-channel summary
```


Muestra el ejemplo

```
cs1-new# 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      Eth1/35(P)  Eth1/36(P)
```

```
cs2-new# 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      Eth1/35(P)  Eth1/36(P)
```

Paso 3: Verificar la configuración

1. Habilite la reversión automática en las LIF del clúster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

2. Compruebe que las LIF del clúster han vuelto a sus puertos raíz (esto puede tardar un minuto):

```
network interface show -vserver Cluster
```

Si los LIF del clúster no han cambiado a su puerto de inicio, los revierte manualmente:

```
network interface revert -vserver Cluster -lif *
```

3. Compruebe que el clúster esté en buen estado:

```
cluster show
```

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y. network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```



Espere unos segundos antes de ejecutar el `show` Comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2_clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
none			

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarla llamando a un mensaje AutoSupport:
`system node autosupport invoke -node * -type all -message MAINT=END`

El futuro

Después de haber migrado los conmutadores, ["configurar la monitorización del estado del conmutador"](#) .

Migre a un clúster de dos nodos con switches

Si tiene un entorno de clúster *sin conmutador* de dos nodos existente, puede migrar a un entorno de clúster *conmutado* de dos nodos utilizando los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T.

El proceso de migración funciona para todos los nodos utilizando puertos ópticos o Twinax, pero no es compatible con este switch si los nodos utilizan puertos RJ45 DE 10 GB BASE-T integrados para los puertos de red de clúster.

Revise los requisitos

Lo que necesitará

- Para la configuración de dos nodos sin switch:
 - La configuración sin switch de dos nodos está correctamente configurada y funciona.

- 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.
- Consulte ["Hardware Universe"](#) Para todas las versiones de ONTAP compatibles.
- Para la configuración de switches Cisco Nexus 9336C-FX2:
 - Ambos switches tienen conectividad de red de gestión.
 - Hay acceso de la consola a los switches de clúster.
 - Las conexiones de switch nodo a nodo y de switch a switch Nexus 9336C-FX2 utilizan cables Twinax o de fibra.

Consulte ["Hardware Universe"](#) para obtener más información sobre el cableado.

- Los cables de enlace entre switches (ISL) están conectados a los puertos 1/35 y 1/36 en los dos switches 9336C-FX2.
- Se completa la personalización inicial de los dos switches 9336C-FX2, para que:
 - Los switches 9336C-FX2 ejecutan la versión más reciente del software.
 - Los archivos de configuración de referencia (RCF) se aplican a los conmutadores. Cualquier personalización del sitio, como SMTP, SNMP y SSH, se configura en los nuevos 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 9336C-FX2 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.

Consulte ["Hardware Universe"](#) para obtener información acerca de los puertos de clúster para las plataformas.

Migrar los switches

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
```

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 Advanced, introduzca `y` cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

Paso 2: Configure los puertos y el cableado

1. Deshabilite todos los puertos orientados a nodos (no los puertos ISL) en los nuevos switches del clúster cs1 y cs2.

No deshabilite los puertos ISL.

Muestra el ejemplo

En el siguiente ejemplo se muestra que los puertos 1 a 34 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 e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs1(config-if-range)# shutdown
```

2. Compruebe que el ISL y los puertos físicos del ISL entre los dos switches 9336C-FX2 cs1 y cs2 estén activos en los puertos 1/35 y 1/36:

```
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      Eth1/35 (P)  Eth1/36 (P)
```

El siguiente ejemplo muestra que los puertos ISL están activos en el switch 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      Eth1/35 (P)  Eth1/36 (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               Eth1/35       175    R S I s         N9K-C9336C
Eth1/35
cs2               Eth1/36       175    R S I s         N9K-C9336C
Eth1/36

Total entries displayed: 2
```

En el siguiente ejemplo se enumeran 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               Eth1/35       177    R S I s         N9K-C9336C
Eth1/35
cs1               Eth1/36       177    R S I s         N9K-C9336C
Eth1/36

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 del clúster debería mostrar 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 del clúster e0a del nodo 1 y, a continuación, conecte e0a al puerto 1 del switch del clúster cs1 mediante el cableado adecuado compatible con los switches 9336C-FX2.

La "[Hardware Universe - interruptores](#)" contiene más información sobre el cableado.

"Hardware Universe - interruptores"

8. Desconecte el cable del puerto e0a del clúster en el nodo 2 y, a continuación, conecte e0a al puerto 2 del switch de clúster cs1 mediante el cableado adecuado compatible con los switches 9336C-FX2.
9. 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 1/34 están habilitados en el conmutador cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs1(config-if-range)# no shutdown
```

10. Compruebe que todas las LIF del clúster estén en funcionamiento, operativas 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 es 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 9336C-FX2.

13. Desconecte el cable del puerto e0b del clúster en el nodo 2 y, a continuación, conecte e0b al puerto 2 del switch cs2 del clúster mediante el cableado adecuado compatible con los switches 9336C-FX2.
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 1/34 están habilitados en el conmutador cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs2(config-if-range)# no shutdown
```

15. 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.

Paso 3: Verificar la configuración

1. 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
```

Current Is	Logical	Status	Network	Current	
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
true					

4 entries were displayed.

2. 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 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs2 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

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 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

Total entries displayed: 4

3. 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-
C9336C
           e0b    cs2                      0/2      N9K-
C9336C
node1      /cdp
           e0a    cs1                      0/1      N9K-
C9336C
           e0b    cs2                      0/1      N9K-
C9336C

4 entries were displayed.
```

4. 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
```

5. 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

6. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

2. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

El futuro

Después de haber migrado sus conmutadores, ["configurar la monitorización del estado del conmutador"](#) .

Reemplace los interruptores

Reemplazar los conmutadores de clúster Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Siga estos pasos para reemplazar los conmutadores Nexus 9336C-FX2 y 9336C-FX2-T defectuosos en una red de clúster. Este es un procedimiento no disruptivo (NDU).

Revise los requisitos

Antes de realizar la sustitución del interruptor, asegúrese de que:

- Ha verificado el número de serie del interruptor para asegurarse de que se sustituye el interruptor correcto.
- 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 son **up**.
 - Todas las interfaces lógicas de cluster (LIF) son **up** y en sus puertos domésticos.
 - La `ONTAP cluster ping-cluster -node node1` El comando debe indicar que la conectividad básica y la comunicación más grande que PMTU son correctas en todas las rutas.
- En el switch de sustitución Nexus 9336C-FX2:
 - 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 1/34.
 - Todos los puertos de enlace entre switches (ISL) están deshabilitados en los puertos 1/35 y 1/36.
 - 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 y como se detalla en ["Configure el switch de clúster 9336C-FX2"](#).

Cualquier personalización de sitio anterior, como STP, SNMP y SSH, se copian al nuevo switch.

- Ha ejecutado el comando para migrar una LIF de clúster desde el nodo en el que se aloja la LIF del clúster.

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después de las tareas de mantenimiento para deshabilitar la creación de casos durante el mantenimiento. Consulte este artículo de la base de conocimientos ["SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#) para obtener más detalles.
- Habilite el registro de sesiones para cualquier sesión de CLI. Para obtener instrucciones sobre cómo activar el registro de sesiones, consulte la sección «Salida de sesión de registro» de este artículo de la base de conocimientos ["Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP"](#).

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 9336C-FX2 existentes son cs1 y cs2.
- El nombre del nuevo switch Nexus 9336C-FX2 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

El siguiente procedimiento se basa en la siguiente topología de red de clúster:

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	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e0a	cs1	Eth1/2	N9K-
C9336C				
	e0b	cs2	Eth1/2	N9K-
C9336C				
node1	/cdp			
	e0a	cs1	Eth1/1	N9K-
C9336C				
	e0b	cs2	Eth1/1	N9K-
C9336C				

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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	144	H	FAS2980	e0a
node2	Eth1/2	145	H	FAS2980	e0a
cs2	Eth1/35	176	R S I s	N9K-C9336C	
Eth1/35					
cs2 (FD0220329V5)	Eth1/36	176	R S I s	N9K-C9336C	
Eth1/36					

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	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	139	H	FAS2980	e0b
node2	Eth1/2	124	H	FAS2980	e0b
cs1	Eth1/35	178	R S I s	N9K-C9336C	
Eth1/35					
cs1	Eth1/36	178	R S I s	N9K-C9336C	
Eth1/36					

```
Total entries displayed: 4
```

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
```

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. 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 Descarga.
 - 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.
3. 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 1/34).

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 e1/1-34
newcs2(config-if-range)# shutdown
```

4. 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.
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
none		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
none		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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 1/35 y 1/36 en el switch Nexus 9336C-FX2 cs1.

Muestra el ejemplo

```

cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/35-36
cs1(config-if-range)# shutdown
cs1(config-if-range)#

```

2. Retire todos los cables del conmutador Nexus 9336C-FX2 cs2 y, a continuación, conéctelos a los mismos puertos del conmutador Nexus C9336C-FX2 newcs2.
3. Traiga los puertos ISL 1/35 y 1/36 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 eth1/35(P) y eth1/36(P).

Muestra el ejemplo

En este ejemplo, se habilitan los puertos ISL 1/35 y 1/36, 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 e1/35-36
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      Eth1/35 (P)  Eth1/36 (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				
e0a	node1_clus1	up/up	169.254.209.69/16	node1
	true			
e0b	node1_clus2	up/up	169.254.49.125/16	node1
	true			
e0a	node2_clus1	up/up	169.254.47.194/16	node2
	true			
e0a	node2_clus2	up/up	169.254.19.183/16	node2
	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

						Speed (Mbps)
Health	Health			Link	MTU	Admin/Oper
Port	IPspace	Broadcast	Domain			
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			Link	MTU	Admin/Oper
Port	IPspace	Broadcast	Domain			
Status	Status					
-----	-----	-----		-----	-----	-----
e0a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

4 entries were displayed.

8. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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 3: Verificar la configuración

1. 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	cs1	0/2	N9K-
C9336C				
	e0b	newcs2	0/2	N9K-
C9336C				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C9336C				
	e0b	newcs2	0/1	N9K-
C9336C				

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	144	H	FAS2980
e0a				
node2	Eth1/2	145	H	FAS2980
e0a				
newcs2	Eth1/35	176	R S I s	N9K-C9336C
Eth1/35				
newcs2	Eth1/36	176	R S I s	N9K-C9336C

Eth1/36

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 Eth1/35	Eth1/35	178	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	178	R S I s	N9K-C9336C

Total entries displayed: 4

2. 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
```

El futuro

Después de haber reemplazado los interruptores, ["configurar la monitorización del estado del conmutador"](#) .

Reemplace los conmutadores de clúster Cisco Nexus 9336C-FX2 y 9336C-FX2-T con conexiones sin conmutador

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.

Antes de empezar

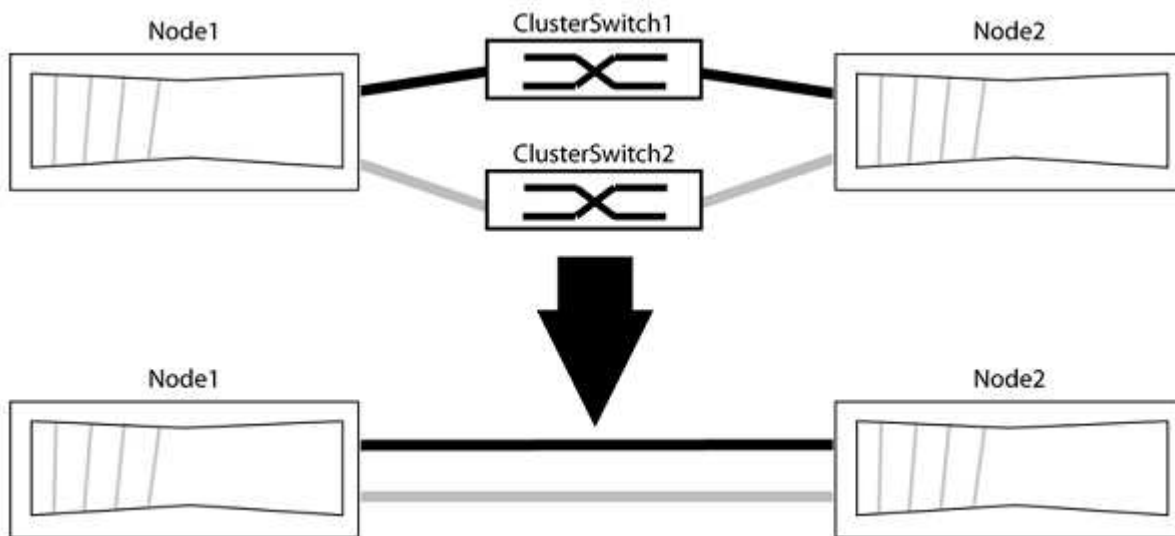
Asegúrese de tener lo siguiente:

- 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

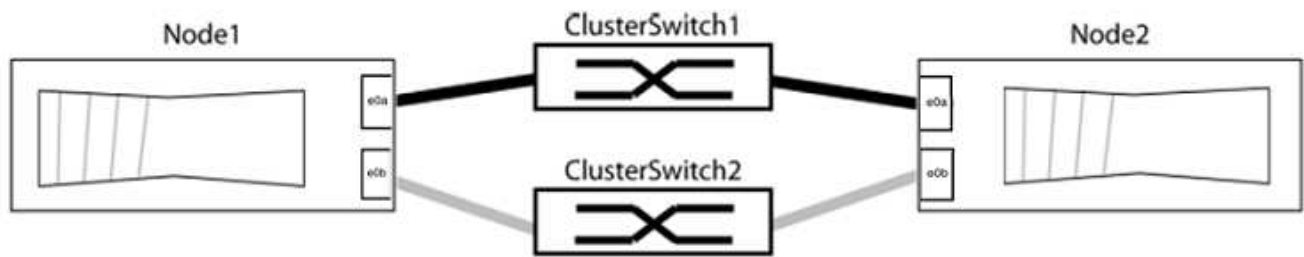
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

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 de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Verifique que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

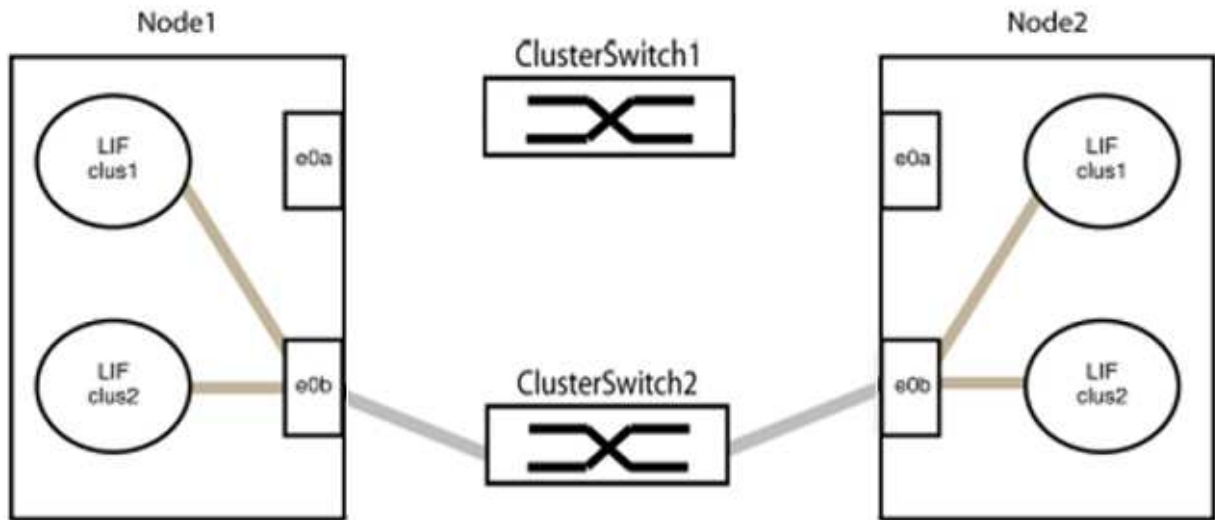
2. Configure la configuración sin switches para los puertos del grupo 1.



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**.

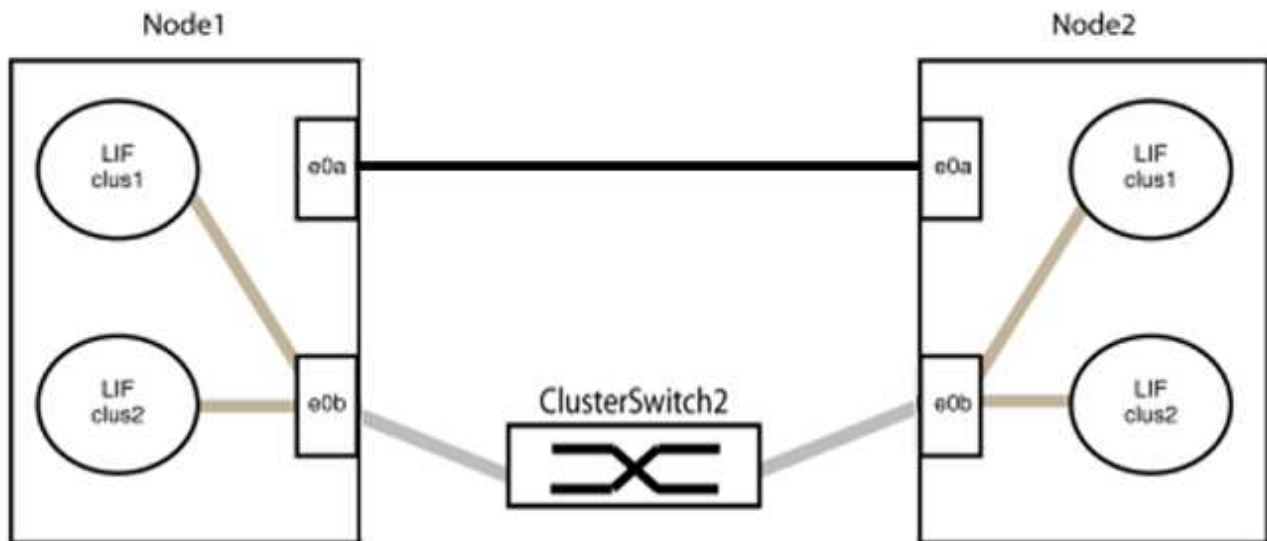
- a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

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:



3. 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
```

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```



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.

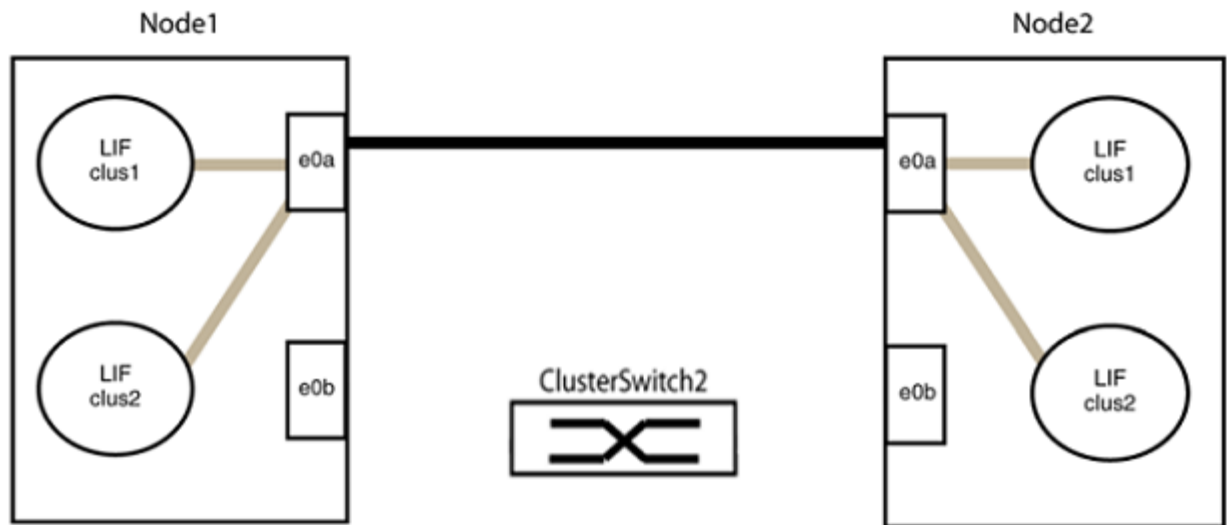
1. Configure la configuración sin switch para los puertos del grupo 2.



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 épsilon en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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"](#).

2. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

NVIDIA SN2100

Manos a la obra

Flujo de trabajo de instalación y configuración para conmutadores NVIDIA SN2100

NVIDIA SN2100 es un switch de clúster que permite crear clústeres de ONTAP con más de dos nodos.

Siga estos pasos de flujo de trabajo para instalar y configurar sus conmutadores NVIDIA SN2100.

1

"Revisar los requisitos de configuración"

Revise los requisitos de configuración para el conmutador de clúster SN2100.

2

"Revise los componentes y números de pieza"

Revise los componentes y números de pieza del conmutador de grupo SN2100.

3

"Revisar la documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores SN2100 y el clúster ONTAP .

4

"Instale el hardware"

Instale el hardware del interruptor.

5

"Configurar el software"

Configurar el software del conmutador.

Requisitos de configuración para los switches NVIDIA SN2100

Para la instalación y el mantenimiento del conmutador NVIDIA SN2100, asegúrese de revisar todos los requisitos de configuración.

Requisitos de instalación

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.

Se instala el switch NVIDIA SN2100 (X190006) en el armario de conmutación doble/simple NVIDIA con los soportes estándar incluidos con el switch.

Para conocer las directrices de cableado, consulte ["Revise las consideraciones sobre el cableado y la configuración"](#).

Soporte de ONTAP y Linux

El conmutador NVIDIA SN2100 es un conmutador 10/25/40/100GbE que ejecuta Cumulus Linux. El conmutador admite lo siguiente:

- ONTAP 9.10.1P3 y versiones posteriores

El switch de SN2100 proporciona aplicaciones de clúster y almacenamiento en ONTAP 9.10.1P3 y versiones posteriores en diferentes pares de switches.

- Versiones de sistema operativo Cumulus Linux (CL)
 - Las versiones específicas de CL están cualificadas y son compatibles con NetApp. Para obtener

información de compatibilidad actual, consulte la ["Información sobre switches Ethernet de NVIDIA"](#) página o el ["Hardware Universe de NetApp"](#).

- Para descargar el software SN2100 Cumulus de NVIDIA, debe tener credenciales de inicio de sesión para acceder al portal de soporte empresarial de NVIDIA. Consulte el artículo de la base de conocimientos ["Cómo registrarse con NVIDIA para el acceso al portal de soporte empresarial"](#).
- Puede instalar Cumulus Linux cuando el conmutador esté ejecutando Cumulus Linux o ONIE.

El futuro

["Componentes y números de pieza"](#).

Componentes y números de pieza para conmutadores NVIDIA SN2100

Para la instalación y el mantenimiento del switch NVIDIA SN2100, asegúrese de revisar la lista de componentes y números de pieza para el kit de armarios y rieles.

Detalles del armario

Se instala el switch NVIDIA SN2100 (X190006) en el armario de conmutación doble/simple NVIDIA con los soportes estándar incluidos con el switch.

Detalles del kit de rieles

La tabla siguiente muestra el número de pieza y la descripción de los interruptores SN2100 y los kits de raíles:

Número de pieza	Descripción
X190006-PE	Cluster Switch, NVIDIA SN2100, 16PT 100GbE, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16PT 100GbE, PSIN
X-MTEF-KIT-D	Kit de rieles, conmutador doble NVIDIA lado a lado
X-MTEF-KIT-E	Kit de rieles, profundidad corta de un único conmutador NVIDIA



Consulte la documentación de NVIDIA para obtener más información acerca de ["Instalación del kit de rieles y interruptor SN2100"](#).

El futuro

["Documentación requerida"](#).

Requisitos de documentación para los switches NVIDIA SN2100

Para la instalación y el mantenimiento del conmutador NVIDIA SN2100, asegúrese de revisar toda la documentación recomendada.

Título	Descripción
"Guía de instalación del switch NVIDIA"	Describe cómo instalar los switches NVIDIA SN2100.

Título	Descripción
"Guía de cableado de bandeja de unidades NVMe NS224"	Información general e ilustraciones que muestran cómo configurar el cableado de bandejas de unidades.
"Hardware Universe de NetApp"	Permite confirmar el hardware compatible, como los switches y cables de almacenamiento, para su modelo de plataforma.

Instale el hardware

Flujo de trabajo de instalación de hardware para conmutadores NVIDIA SN2100

Para instalar y configurar el hardware de un conmutador de clúster SN2100, siga estos pasos:

1 ["Instale el hardware"](#)

Instale el hardware del interruptor.

2 ["Revise las consideraciones sobre el cableado y la configuración"](#)

Revise los requisitos para las conexiones ópticas, el adaptador QSA y la velocidad del puerto de conmutación.

3 ["Conecte el cable de las bandejas NS224"](#)

Siga los procedimientos de cableado si dispone de un sistema en el que las bandejas de unidades NS224 deban cablearse como almacenamiento conectado a switch (no como almacenamiento de conexión directa).

Instale la tornillería del conmutador NVIDIA SN2100

Para instalar el hardware SN2100, consulte la documentación de NVIDIA.

Pasos

1. Revise la ["requisitos de configuración"](#).
2. Siga las instrucciones de ["Guía de instalación del switch NVIDIA"](#).

El futuro

["Revisar el cableado y la configuración"](#) .

Revise las consideraciones sobre el cableado y la configuración

Antes de configurar el conmutador NVIDIA SN2100, revise las siguientes consideraciones.

Detalles del puerto NVIDIA

Puertos del conmutador	Uso de puertos

swp1s0-3	4 nodos de puertos de clúster de 10 GbE de arranque
swp2s0-3	4 nodos de puertos de clúster de 10 GbE de cable abierto
swp3-14	Nodos de puertos de clúster 40/100GbE
swp15-16	100GbE puertos de enlace entre switches (ISL)

Consulte "[Hardware Universe](#)" para obtener más información sobre los puertos de switch.

Retrasos de conexión con conexiones ópticas

Si experimenta retrasos de enlace de más de cinco segundos, Cumulus Linux 5,4 y posterior incluye soporte para conexión rápida. Puede configurar los enlaces mediante `nv set` comando de la siguiente manera:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Muestra el ejemplo

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Soporte para conexiones de cobre

Se requieren los siguientes cambios de configuración para solucionar este problema.

Cumulus Linux 4.4.3

1. Identifique el nombre de cada interfaz mediante cables de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
```

Interface Vendor Rev	Identifier	Vendor Name	Vendor PN	Vendor SN
----- -----	-----	-----	-----	-----
swp3 B0	0x11 (QSFP28)	Molex	112-00576	93A2229911111
swp4 B0	0x11 (QSFP28)	Molex	112-00576	93A2229922222

2. Añada las dos líneas siguientes a la `/etc/cumulus/switchd.conf` Archivo para cada puerto (swp<n>) que utilice cables de cobre 40GbE/100GbE:

- `interface.swp<n>.enable_media_depended_linkup_flow=TRUE`
- `interface.swp<n>.enable_short_tuning=TRUE`

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
.
.
interface.swp3.enable_media_depended_linkup_flow=TRUE
interface.swp3.enable_short_tuning=TRUE
interface.swp4.enable_media_depended_linkup_flow=TRUE
interface.swp4.enable_short_tuning=TRUE
```

3. Reinicie el `switchd` servicio:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Confirme que los puertos están activos:

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp3	100G	9216	Trunk/L2		Master: bridge(UP)
UP	swp4	100G	9216	Trunk/L2		Master: bridge(UP)

Cumulus Linux 5.x

1. Identifique el nombre de cada interfaz mediante cables de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ nv show interface --view=pluggables
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor SN
swp3	0x11 (QSFP28)	Molex	112-00576	93A2229911111
B0				
swp4	0x11 (QSFP28)	Molex	112-00576	93A2229922222
B0				

2. Configure los enlaces mediante `nv set` comando de la siguiente manera:

- ° `nv set interface <interface-id> link fast-linkup on`
- ° `nv config apply`
- ° Vuelva a cargar el `switchd` servicio

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

3. Confirme que los puertos están activos:

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp3	100G	9216	Trunk/L2		Master: bridge(UP)
UP	swp4	100G	9216	Trunk/L2		Master: bridge(UP)

Consulte el artículo de la base de conocimientos ["El switch SN2100 no se puede conectar mediante cables de cobre de 40/100GbE"](#) para obtener más información.

En Cumulus Linux 4.4.2, las conexiones de cobre no son compatibles con los switches SN2100 con X1151A NIC, X1146A NIC o 100GbE puertos integrados. Por ejemplo:

- AFF A800 en los puertos e0a y e0b
- AFF A320 en los puertos e0g y e0h

Adaptador QSA

Cuando se utiliza un adaptador QSA para conectarse a los puertos de clúster 10GbE/25GbE en una plataforma, es posible que el enlace no aparezca.

Para resolver este problema, haga lo siguiente:

- Para 10GbE, ajuste manualmente la velocidad de enlace swp1s0-3 a 10000 y establezca la negociación automática en OFF.
- Para 25GbE, ajuste manualmente la velocidad de enlace swp2s0-3 a 25000 y establezca la negociación automática en OFF.



Cuando utilice adaptadores QSA de 10GbE/25GbE, insértelos en puertos 40GbE/100GbE que no sean separables (swp3-swp14). No inserte el adaptador QSA en un puerto configurado para la desconexión.

Configuración de la velocidad de la interfaz en los puertos de arranque

Dependiendo del transceptor en el puerto del switch, es posible que necesite configurar la velocidad en la interfaz del switch a una velocidad fija. Si utiliza puertos de desconexión 10GbE y 25GbE, verifique que la negociación automática esté desactivada y establezca la velocidad de la interfaz en el switch.

Cumulus Linux 4.4.3

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces      2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp1s3
iface swp1s3
    alias 10G Intra-Cluster Node
-   link-autoneg off
+   link-autoneg on
    link-speed 10000 <---- port speed set
    mstpctl-bpduguard yes
    mstpctl-portadminedge yes
    mtu 9216

auto swp2s0
iface swp2s0
    alias 25G Intra-Cluster Node
    link-autoneg off
    link-speed 25000 <---- port speed set
```

Compruebe el estado de la interfaz y del puerto para verificar que se aplican los ajustes:

```
cumulus@cumulus:mgmt:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	
.						
.						
UP	swp1s0	10G	9216	Trunk/L2	cs07 (e4c)	Master:
br_default(UP)						
UP	swp1s1	10G	9216	Trunk/L2	cs07 (e4d)	Master:
br_default(UP)						
UP	swp1s2	10G	9216	Trunk/L2	cs08 (e4c)	Master:
br_default(UP)						
UP	swp1s3	10G	9216	Trunk/L2	cs08 (e4d)	Master:
br_default(UP)						
.						
.						
UP	swp3	40G	9216	Trunk/L2	cs03 (e4e)	Master:
br_default(UP)						
UP	swp4	40G	9216	Trunk/L2	cs04 (e4e)	Master:
br_default(UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
br_default(UP)						
.						
.						
UP	swp15	100G	9216	BondMember	cs01 (swp15)	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	cs01 (swp16)	Master:
cluster_isl(UP)						
.						
.						

Cumulus Linux 5.x

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3
```

```
link
```

auto-negotiate	off	off
duplex	full	full
speed	10G	10G
fec	auto	auto
mtu	9216	9216
[breakout]		
state	up	up

Compruebe el estado de la interfaz y del puerto para verificar que se aplican los ajustes:

```
cumulus@cumulus:mgmt:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	
.						
.						
UP	swp1s0	10G	9216	Trunk/L2	cs07 (e4c)	Master:
br_default(UP)						
UP	swp1s1	10G	9216	Trunk/L2	cs07 (e4d)	Master:
br_default(UP)						
UP	swp1s2	10G	9216	Trunk/L2	cs08 (e4c)	Master:
br_default(UP)						
UP	swp1s3	10G	9216	Trunk/L2	cs08 (e4d)	Master:
br_default(UP)						
.						
.						
UP	swp3	40G	9216	Trunk/L2	cs03 (e4e)	Master:
br_default(UP)						
UP	swp4	40G	9216	Trunk/L2	cs04 (e4e)	Master:
br_default(UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
br_default(UP)						
.						
.						
UP	swp15	100G	9216	BondMember	cs01 (swp15)	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	cs01 (swp16)	Master:
cluster_isl(UP)						
.						
.						

El futuro

"Conecte el cable de las bandejas NS224 como almacenamiento conectado al conmutador".

Conecte el cable de las bandejas NS224 como almacenamiento conectado al switch

Si tiene un sistema en el que las bandejas de unidades NS224 deben cablearse como almacenamiento conectado al switch (no como almacenamiento de conexión directa), utilice la información proporcionada aquí.

- Conectar las bandejas de unidades NS224 a través de switches de almacenamiento:

["Cableado de bandejas de unidades NS224 conectadas a switch"](#)

- Confirme el hardware compatible, como los switches y cables de almacenamiento, para su modelo de plataforma:

["Hardware Universe de NetApp"](#)

El futuro

["Configure el switch"](#).

Configurar el software

Flujo de trabajo de instalación de software para los switches NVIDIA SN2100

Para instalar y configurar el software para un conmutador NVIDIA SN2100, siga estos pasos:

1

["Configure el switch"](#)

Configurar el conmutador NVIDIA SN2100.

2

["Instale Cumulus Linux en modo Cumulus"](#)

Puede instalar el sistema operativo Cumulus Linux (CL) cuando el conmutador ejecuta Cumulus Linux.

3

["Instale Cumulus Linux en modo ONIE"](#)

Como alternativa, puede instalar el sistema operativo Cumulus Linux (CL) cuando el conmutador ejecuta Cumulus Linux en modo ONIE.

4

["Actualice su versión de Cumulus Linux, según sea necesario"](#)

Puede actualizar su sistema operativo Cumulus Linux (CL) según sea necesario.

5

["Instale o actualice el script Reference Configuration File \(RCF\)"](#)

Hay dos secuencias de comandos RCF disponibles para las aplicaciones de almacenamiento y agrupación en clúster. El procedimiento para cada uno es el mismo.

6

["Instale el archivo CSHM"](#)

Puede instalar el archivo de configuración correspondiente para la supervisión del estado del switch Ethernet de los switches de clúster de NVIDIA.

7

"Restablecer el interruptor a los valores predeterminados de fábrica"

Borre la configuración del interruptor del grupo SN2100.

Configure el conmutador NVIDIA SN2100

Para configurar el conmutador SN2100, consulte la documentación de NVIDIA.

Pasos

1. Revise la ["requisitos de configuración"](#).
2. Siga las instrucciones de ["Puesta en marcha del sistema NVIDIA."](#).

El futuro

["Instale Cumulus Linux en modo Cumulus"](#) o ["Instale Cumulus Linux en modo ONIE"](#).

Instale Cumulus Linux en modo Cumulus

Siga este procedimiento para instalar Cumulus Linux (CL) OS cuando el conmutador se esté ejecutando en modo Cumulus.



Cumulus Linux (CL) OS se puede instalar ya sea cuando el conmutador ejecuta Cumulus Linux o ONIE (consulte ["Instale EN modo ONIE"](#)).

Antes de empezar

Asegúrese de tener lo siguiente:

- Conocimientos de Linux de nivel intermedio.
- Estar familiarizado con la edición de texto básica, los permisos de archivos UNIX y la supervisión de procesos. Una variedad de editores de texto están preinstalados, incluyendo `vi` y `nano`.
- Acceso a un shell de Linux o UNIX. Si ejecuta Windows, utilice un entorno Linux como herramienta de línea de comandos para interactuar con Cumulus Linux.
- El requisito de velocidad en baudios se establece en 115200 en el conmutador de consola serie para el acceso a la consola del conmutador NVIDIA SN2100 de la siguiente manera:
 - 115200 baudios
 - 8 bits de datos
 - 1 bit de parada
 - paridad: none
 - control de flujo: ninguno

Acerca de esta tarea

Tenga en cuenta lo siguiente:



Cada vez que se instala Cumulus Linux, se borra y reconstruye toda la estructura del sistema de archivos.



La contraseña predeterminada para la cuenta de usuario de cumulus es **cumulus**. La primera vez que inicie sesión en Cumulus Linux, debe cambiar esta contraseña predeterminada. Asegúrese de actualizar cualquier secuencia de comandos de automatización antes de instalar una nueva imagen. Cumulus Linux proporciona opciones de línea de comandos para cambiar automáticamente la contraseña predeterminada durante el proceso de instalación.

Ejemplo 1. Pasos

Cumulus Linux 4.4.3

1. Inicie sesión en el switch.

La primera vez que inicia sesión en el conmutador requiere nombre de usuario/contraseña de **cumulus/cumulus** con sudo privilegios.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Compruebe la versión de Cumulus Linux: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo se inicia después de reiniciar la sesión de la consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz se utiliza específicamente para la gestión fuera de banda. De forma predeterminada, la interfaz de gestión utiliza DHCPv4 para la direccionamiento.



No utilice caracteres de subrayado (_), apóstrofe (') o no ASCII en el nombre de host.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Este comando modifica ambos `/etc/hostname` y `/etc/hosts` archivos.

4. Confirme que se han actualizado el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Establezca la fecha, la hora, la zona horaria y el servidor NTP en el switch.

- a. Compruebe la zona horaria actual:

```
cumulus@sw1:~$ cat /etc/timezone
```

- b. Actualizar a la nueva zona horaria:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

c. Verifique su zona horaria actual:

```
cumulus@switch:~$ date +%Z
```

d. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Ajuste el reloj del software según la zona horaria configurada:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Ajuste el valor actual del reloj del software en el reloj del hardware:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>  
iburst  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

h. Compruebe que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp  
ntp          4074      1   0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p  
/var/run/ntpd.pid -g -u 101:102
```

i. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que usa NTP es eth0. Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ net add time ntp source <src_int>  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

6. Instale Cumulus Linux 4.4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el conmutador NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones de pantalla de GRUB. * No* realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar el sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Compruebe que la versión de Cumulus Linux es 4.4.3: `net show version`

```
cumulus@sw1:mgmt:~$ net show version  
NCLU_VERSION=1.0-cl4.4.3u0  
DISTRIB_ID="Cumulus Linux"  
DISTRIB_RELEASE=4.4.3  
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Cree un nuevo usuario y agregue este usuario a `sudo` grupo. Este usuario sólo se hace efectivo después de reiniciar la sesión de la consola/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

Cumulus Linux 5.4.0

1. Inicie sesión en el switch.

La primera vez que inicia sesión en el conmutador requiere nombre de usuario/contraseña de

cumulus/cumulus con sudo privilegios.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Compruebe la versión de Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.3.0	system build version
uptime	6 days, 8:37:36	system uptime
timezone	Etc/UTC	system time zone

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo se inicia después de reiniciar la sesión de la consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz se utiliza específicamente para la gestión fuera de banda. De forma predeterminada, la interfaz de gestión utiliza DHCPv4 para la direccionamiento.



No utilice caracteres de subrayado (`_`), apóstrofe (`'`) o no ASCII en el nombre de host.

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica ambos `/etc/hostname` y `/etc/hosts` archivos.

4. Confirme que se han actualizado el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

```

cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1

```

5. Establezca la zona horaria, la fecha, la hora y el servidor NTP en el switch.

a. Establezca la zona horaria:

```

cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply

```

b. Verifique su zona horaria actual:

```

cumulus@switch:~$ date +%Z

```

c. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```

cumulus@sw1:~$ sudo dpkg-reconfigure tzdata

```

d. Ajuste el reloj del software según la zona horaria configurada:

```

cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"

```

e. Ajuste el valor actual del reloj del software en el reloj del hardware:

```

cumulus@sw1:~$ sudo hwclock -w

```

f. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Consulte el artículo de la base de conocimientos ["La configuración del servidor NTP no funciona con los conmutadores NVIDIA SN2100"](#) Para más detalles.

g. Compruebe que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp          4074      1  0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que usa NTP es eth0. Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instale Cumulus Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el conmutador NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones de pantalla de GRUB. * No* realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar el sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Compruebe que la versión de Cumulus Linux es 5.4.0: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	system build version
uptime	6 days, 13:37:36	system uptime
timezone	Etc/UTC	system time zone

11. Compruebe que cada nodo tenga una conexión con cada switch:

```
cumulus@sw1:mgmt:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost
RemotePort			
eth0	100M	Mgmt	mgmt-sw1
Eth110/1/29			
swp2s1	25G	Trunk/L2	node1
e0a			
swp15	100G	BondMember	sw2
swp15			
swp16	100G	BondMember	sw2
swp16			

12. Cree un nuevo usuario y agregue este usuario a sudo grupo. Este usuario sólo se hace efectivo después de reiniciar la sesión de la consola/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

13. Agregue grupos de usuarios adicionales al que pueda acceder el usuario administrador `nv` comandos:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user 'admin' to group 'nvshow' ...
Adding user admin to group nvshow
Done.
```

Consulte ["Cuentas de usuario de NVIDIA"](#) si quiere más información.

Cumulus Linux 5.11.0

1. Inicie sesión en el switch.

Cuando inicia sesión en el conmutador por primera vez, requiere el nombre de usuario/contraseña de **cumulus/cumulus** con sudo Privileges.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Compruebe la versión de Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	system build version
uptime	6 days, 8:37:36	system uptime
timezone	Etc/UTC	system time zone

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo se inicia después de reiniciar la sesión de la consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz se utiliza específicamente para la gestión fuera de banda. De forma predeterminada, la interfaz de gestión utiliza DHCPv4 para la direccionamiento.



No utilice caracteres de subrayado (`_`), apóstrofe (`'`) o no ASCII en el nombre de host.

```
cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica ambos `/etc/hostname` y `/etc/hosts` archivos.

4. Confirme que se han actualizado el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Establezca la zona horaria, la fecha, la hora y el servidor NTP en el switch.

- a. Establezca la zona horaria:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

- b. Verifique su zona horaria actual:

```
cumulus@switch:~$ date +%Z
```

- c. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

- d. Ajuste el reloj del software según la zona horaria configurada:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

- e. Ajuste el valor actual del reloj del software en el reloj del hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

- f. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Consulte el artículo de la base de conocimientos ["La configuración del servidor NTP no funciona con los conmutadores NVIDIA SN2100"](#) Para más detalles.

- g. Compruebe que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp          4074      1   0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

- h. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que usa NTP es eth0. Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instale Cumulus Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el conmutador NVIDIA SN2100:


```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones de pantalla de GRUB. * No* realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar el sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Compruebe que la versión de Cumulus Linux es 5.11.0:

```
nv show system
```

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
build	Cumulus Linux 5.11.0	
uptime	153 days, 2:44:16	
hostname	cumulus	cumulus
product-name	Cumulus Linux	
product-release	5.11.0	
platform	x86_64-mlnx_x86-r0	
system-memory	2.76 GB used / 2.28 GB free / 7.47 GB total	
swap-memory	0 Bytes used / 0 Bytes free / 0 Bytes total	
health-status	not OK	
date-time	2025-04-23 09:55:24	
status	N/A	
timezone	Etc/UTC	
maintenance		
mode	disabled	
ports	enabled	
version		
kernel	6.1.0-cl-1-amd64	
build-date	Thu Nov 14 13:06:38 UTC 2024	
image	5.11.0	
onie	2019.11-5.2.0020-115200	

11. Compruebe que cada nodo tenga una conexión con cada switch:

```
cumulus@sw1:mgmt:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost
RemotePort			

eth0	100M	eth	mgmt-sw1
Eth110/1/14			
swp2s1	25G	Trunk/L2	node1
e0a			
swp1s1	10G	swp	sw2
e0a			
swp9	100G	swp	sw3
e4a			
swp10	100G	swp	sw4
e4a			
swp15	100G	swp	sw5
swp15			
swp16	100G	swp	sw6
swp16			

Consulte ["Cuentas de usuario de NVIDIA"](#) para obtener más información.

El futuro

["Instale la secuencia de comandos del archivo de configuración de referencia \(RCF\)".](#)

Instale Cumulus Linux en modo ONIE

Siga este procedimiento para instalar Cumulus Linux (CL) OS cuando el conmutador se ejecute EN modo ONIE.



Cumulus Linux (CL) OS se puede instalar ya sea cuando el conmutador ejecuta ONIE o Cumulus Linux (consulte ["Instalar en modo Cumulus"](#)).

Acerca de esta tarea

Puede instalar Cumulus Linux utilizando Open Network Install Environment (ONIE) que permite la detección automática de una imagen de instalador de red. Esto facilita el modelo de sistema de asegurar los conmutadores con una opción de sistema operativo, como Cumulus Linux. La forma más fácil de instalar Cumulus Linux con ONIE es con el descubrimiento HTTP local.



Si el host tiene IPv6 habilitada, asegúrese de que ejecuta un servidor web. Si el host tiene la función IPv4 habilitada, asegúrese de que esté ejecutando DHCP además de un servidor web.

Este procedimiento muestra cómo actualizar Cumulus Linux después de que el administrador haya arrancado EN ONIE.

Ejemplo 2. Pasos

Cumulus Linux 4.4.3

1. Descargue el archivo de instalación de Cumulus Linux en el directorio raíz del servidor Web. Cambie el nombre de este archivo a: `onie-installer`.
2. Conecte el host al puerto Ethernet de gestión del switch mediante un cable Ethernet.
3. Encienda el interruptor.

El conmutador descarga el instalador DE imágenes ONIE y arranca. Una vez finalizada la instalación, aparece el indicador de inicio de sesión de Cumulus Linux en la ventana del terminal.



Cada vez que se instala Cumulus Linux, se borra y reconstruye toda la estructura del sistema de archivos.

4. Reinicie el interruptor SN2100:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

5. Pulse la tecla **Esc** en la pantalla GNU GRUB para interrumpir el proceso de arranque normal, seleccione **ONIE** y pulse **Intro**.
6. En la siguiente pantalla, seleccione **ONIE: Install OS**.
7. EL proceso DE detección DEL instalador DE ONIE ejecuta la búsqueda de la instalación automática. Pulse **Intro** para detener temporalmente el proceso.
8. Cuando el proceso de detección se detuvo:

```
ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover...start-stop-daemon: warning: killing process
427:
No such process done.
```

9. Si el servicio DHCP se está ejecutando en la red, compruebe que la dirección IP, la máscara de subred y la puerta de enlace predeterminada están correctamente asignadas:

```
ifconfig eth0
```

```

ONIE:/ # ifconfig eth0
eth0    Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
        inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
        inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
        TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
        Memory:dfc00000-dfc1ffff

```

```

ONIE:/ # route
Kernel IP routing table

```

Destination	Gateway	Genmask	Flags	Metric	Ref
Use Iface					
default	10.233.204.1	0.0.0.0	UG	0	0
0 eth0					
10.233.204.0	*	255.255.254.0	U	0	0
0 eth0					

10. Si el esquema de direccionamiento IP se define manualmente, haga lo siguiente:

```

ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1

```

11. Repita el paso 9 para comprobar que la información estática se ha introducido correctamente.

12. Instalar Cumulus Linux:

```

# onie-nos-install http://<web-server>/<path>/cumulus-linux-4.4.3-
mlx-amd64.bin

```

```

ONIE:/ # route

Kernel IP routing table

ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-4.4.3-mlx-amd64.bin

Stopping: discover... done.
Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-
4.4.3-mlx-amd64.bin ...
Connecting to 10.60.132.97 (10.60.132.97:80)
installer          100% |*|    552M  0:00:00 ETA
...
...

```

13. Una vez completada la instalación, inicie sesión en el switch.

```

cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>

```

14. Verifique la versión de Cumulus Linux: `net show version`

```

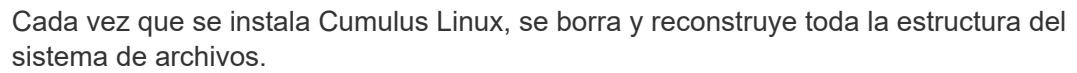
cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"

```

Cumulus Linux 5.x

1. Descargue el archivo de instalación de Cumulus Linux en el directorio raíz del servidor Web. Cambie el nombre de este archivo a: `onie-installer`.
2. Conecte el host al puerto Ethernet de gestión del switch mediante un cable Ethernet.
3. Encienda el interruptor.

El conmutador descarga el instalador DE imágenes ONIE y arranca. Una vez finalizada la instalación, aparece el indicador de inicio de sesión de Cumulus Linux en la ventana del terminal.



4. Reinicie el interruptor SN2100:

[illegible]

5. Presione la tecla Esc en la pantalla de GNU GRUB para interrumpir el proceso de inicio normal, seleccione ONIE y presione Intro.

```

.
.
Loading ONIE ...

GNU GRUB version 2.02
+-----+
-----+
| ONIE: Install OS
|
| ONIE: Rescue
|
| ONIE: Uninstall OS
|
| ONIE: Update ONIE
|
| ONIE: Embed ONIE
|
|
|
|
|
|
|
|
|
|
|
+-----+
-----+

```

Seleccione ONIE: **Instalar OS**.

6. EL proceso DE detección DEL instalador DE ONIE ejecuta la búsqueda de la instalación automática. Pulse **Intro** para detener temporalmente el proceso.
7. Cuando el proceso de detección se detuvo:

```

ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover...start-stop-daemon: warning: killing process
427:
No such process done.

```

8. Configure la dirección IP, la máscara de subred y la puerta de enlace predeterminada:

```
ifconfig eth0
```

```

ONIE:/ # ifconfig eth0
eth0    Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
        inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
        inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
        TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
        Memory:dfc00000-dfc1ffff

ONIE:/ #
ONIE:/ # ifconfig eth0 10.228.140.27 netmask 255.255.248.0
ONIE:/ # ifconfig eth0
eth0    Link encap:Ethernet HWaddr B8:CE:F6:5E:05:E6
        inet addr:10.228.140.27 Bcast:10.228.143.255
Mask:255.255.248.0
        inet6 addr: fd20:8b1e:b255:822b:bace:f6ff:fe5e:5e6/64
Scope:Global
        inet6 addr: fe80::bace:f6ff:fe5e:5e6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:18813 errors:0 dropped:1418 overruns:0 frame:0
        TX packets:491 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1339596 (1.2 MiB) TX bytes:49379 (48.2 KiB)
        Memory:dfc00000-dfc1ffff

ONIE:/ # route add default gw 10.228.136.1
ONIE:/ # route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref
Use Iface

default          10.228.136.1    0.0.0.0          UG      0      0
0 eth0
10.228.136.1     *               255.255.248.0    U        0      0
0 eth0

```

9. Instalar Cumulus Linux 5,4:

```
# onie-nos-install http://<web-server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```



```

ONIE:/ # route

Kernel IP routing table

ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-5.4-mlx-amd64.bin

Stopping: discover... done.
Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-5.4-
mlx-amd64.bin ...
Connecting to 10.60.132.97 (10.60.132.97:80)
installer          100% |*|    552M  0:00:00 ETA
...
...

```

10. Una vez completada la instalación, inicie sesión en el switch.

```

cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>

```

11. Verifique la versión de Cumulus Linux: `nv show system`

```

cumulus@cumulus:mgmt:~$ nv show system
operational      applied          description
-----
hostname         cumulus         cumulus
build            Cumulus Linux 5.4.0  system build version
uptime           6 days, 13:37:36  system uptime
timezone         Etc/UTC         system time zone

```

12. Cree un nuevo usuario y agregue este usuario a sudo grupo. Este usuario sólo se hace efectivo después de reiniciar la sesión de la consola/SSH.

```

sudo adduser --ingroup netedit admin

```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

13. Agregue grupos de usuarios adicionales al que pueda acceder el usuario administrador `nv` comandos:

```
cumulus@cumulus:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Consulte ["Cuentas de usuario de NVIDIA"](#) si quiere más información.

El futuro

["Instale la secuencia de comandos del archivo de configuración de referencia \(RCF\)".](#)

Actualice las versiones de Cumulus Linux

Complete el siguiente procedimiento para actualizar la versión de Cumulus Linux según sea necesario.

Antes de empezar

Asegúrese de tener lo siguiente:

- Conocimientos de Linux de nivel intermedio.
- Estar familiarizado con la edición de texto básica, los permisos de archivos UNIX y la supervisión de procesos. Una variedad de editores de texto están preinstalados, incluyendo `vi` y `nano`.
- Acceso a un shell de Linux o UNIX. Si ejecuta Windows, utilice un entorno Linux como herramienta de línea de comandos para interactuar con Cumulus Linux.
- El requisito de velocidad en baudios se establece en 115200 en el conmutador de consola serie para el acceso a la consola del conmutador NVIDIA SN2100 de la siguiente manera:
 - 115200 baudios
 - 8 bits de datos
 - 1 bit de parada
 - paridad: none
 - control de flujo: ninguno

Acerca de esta tarea

Tenga en cuenta lo siguiente:



Cada vez que se actualiza Cumulus Linux, se borra y reconstruye toda la estructura del sistema de archivos. La configuración existente se borrará. Debe guardar y registrar la configuración del switch antes de actualizar Cumulus Linux.



La contraseña predeterminada para la cuenta de usuario de cumulus es **cumulus**. La primera vez que inicie sesión en Cumulus Linux, debe cambiar esta contraseña predeterminada. Debe actualizar todos los scripts de automatización antes de instalar una imagen nueva. Cumulus Linux proporciona opciones de línea de comandos para cambiar automáticamente la contraseña predeterminada durante el proceso de instalación.

Consulte ["Instalación de una nueva imagen de Cumulus Linux"](#) para obtener más información.

Ejemplo 3. Pasos

Cumulus Linux 4.4.x a Cumulus Linux 5.4.0

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el comando ping para verificar la conectividad con el servidor que aloja Cumulus Linux y el RCF.
3. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```

4. 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
```

- b. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

```
network interface show -role cluster
```

- c. Compruebe que el clúster muestra información de ambos switches de clúster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

6. Compruebe la versión actual de Cumulus Linux y los puertos conectados:

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

```
cumulus@cumulus:mgmt:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

.					
.					
UP	swp1	100G	9216	Trunk/L2	node1 (e5b)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e5b)
Master: bridge(UP)					
UP	swp3	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp5	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
UP	swp6	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
.					
.					

7. Descargue la imagen de Cumulux Linux 5.4.0:

```
cumulus@cumulus:mgmt:~$ sudo onie-install -a -i http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Reinicie el switch:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

9. Cambie la contraseña:

```

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

```

10. Compruebe la versión de Cumulus Linux: `nv show system`

```

cumulus@cumulus:mgmt:~$ nv show system

```

	operational	applied
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	
uptime	14:07:08	
timezone	Etc/UTC	

11. Cambie el nombre de host:

```

cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/syncd/syncd.conf
.
.

```

12. Cierre la sesión e inicie sesión en el conmutador de nuevo para ver el nombre del conmutador actualizado en el prompt:


```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Establezca la dirección IP:

```
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Cree un nuevo usuario y agregue este usuario a sudo grupo. Este usuario sólo se hace efectivo después de reiniciar la sesión de la consola/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

15. Agregue grupos de usuarios adicionales al que pueda acceder el usuario administrador `nv` comandos:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Consulte ["Cuentas de usuario de NVIDIA"](#) si quiere más información.

Cumulus Linux 5.x a Cumulus Linux 5.4.0

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el comando ping para verificar la conectividad con el servidor que aloja Cumulus Linux y el RCF.
3. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```

4. 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
```

- b. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

```
network interface show -role cluster
```

- c. Compruebe que el clúster muestra información de ambos switches de clúster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

6. Compruebe la versión actual de Cumulus Linux y los puertos conectados:

```

cumulus@sw1:mgmt:~$ nv show system
                                operational          applied
-----
hostname                        cumulus              cumulus
build                          Cumulus Linux 5.3.0
uptime                         6 days, 8:37:36
timezone                       Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----
+ cluster_isl  9216  200G  up
bond
+ eth0          1500  100M  up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo            65536      up
loopback      IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0        9216  10G   up    cluster01         e0b
swp
.
.
.
+ swp15         9216  100G   up    sw2                swp15
swp
+ swp16         9216  100G   up    sw2                swp16
swp

```

7. Descargue la imagen de Cumulux Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Reinicie el switch:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

9. Cambie la contraseña:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Compruebe la versión de Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational      applied
-----
hostname         cumulus cumulus
build            Cumulus Linux 5.4.0
uptime          14:07:08
timezone         Etc/UTC
```

11. Cambie el nombre de host:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/syncd/syncd.conf
.
.
```

12. Cierre la sesión y vuelva a iniciar sesión en el conmutador para ver el nombre del conmutador actualizado en el prompt:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Establezca la dirección IP:

```
cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Cree un nuevo usuario y agregue este usuario a sudo grupo. Este usuario sólo se hace efectivo después de reiniciar la sesión de la consola/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

15. Agregue grupos de usuarios adicionales al que pueda acceder el usuario administrador `nv` comandos:


```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Consulte ["Cuentas de usuario de NVIDIA"](#) si quiere más información.

Cumulus Linux 5.4.0 a Cumulus Linux 5.11.0

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el comando ping para verificar la conectividad con el servidor que aloja Cumulus Linux y el RCF.
3. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```

4. 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
```

- b. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

```
network interface show -role cluster
```

- c. Compruebe que el clúster muestra información de ambos switches de clúster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

6. Compruebe la versión actual de Cumulus Linux y los puertos conectados:

```

cumulus@sw1:mgmt:~$ nv show system
                                operational          applied
-----
hostname                        cumulus              cumulus
build                          Cumulus Linux 5.4.0
uptime                         6 days, 8:37:36
timezone                       Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----
+ cluster_isl  9216  200G  up
bond
+ eth0         1500  100M  up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo           65536      up
loopback      IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0       9216  10G   up    cluster01         e0b
swp
.
.
.
+ swp15        9216  100G   up    sw2                swp15
swp
+ swp16        9216  100G   up    sw2                swp16
swp

```

7. Descargue la imagen de Cumulux Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Reinicie el switch:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

9. Cambie la contraseña:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Compruebe la versión de Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational      applied
-----
hostname         cumulus cumulus
build            Cumulus Linux 5.11.0
uptime          14:07:08
timezone         Etc/UTC
```

11. Cambie el nombre de host:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/syncd/syncd.conf
.
.
```

12. Cierre sesión y vuelva a iniciar sesión en el conmutador para ver el nombre del conmutador actualizado en el mensaje:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Establezca la dirección IP:

```
cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

El futuro

["Instale o actualice el script RCF"](#).

Instale o actualice el script Reference Configuration File (RCF)

Siga este procedimiento para instalar o actualizar el script RCF.

Antes de empezar

Antes de instalar o actualizar la secuencia de comandos RCF, asegúrese de que los siguientes elementos están disponibles en el conmutador:

- Está instalado Cumulus Linux. Consulte ["Hardware Universe"](#) para las versiones compatibles.

- Dirección IP, máscara de subred y puerta de enlace predeterminada definida a través de DHCP o configurado manualmente.



Debe especificar un usuario en el RCF (además del usuario administrador) para que se utilice específicamente para la recopilación de registros.

Configuraciones del cliente

Están disponibles las siguientes categorías de configuración de referencia:

Clúster	En los puertos configurados para una conexión de 4 x 10 GbE, un puerto está configurado para una conexión de 4 x 25 GbE y los otros puertos están configurados para 40/100 GbE. Admite tráfico de clúster/HA compartido en puertos para nodos que utilizan puertos de clúster/HA compartidos. Consulte la tabla de plataformas en el artículo de la Base de conocimientos " ¿Qué plataformas AFF, ASA y FAS utilizan puertos Ethernet de alta disponibilidad y de clúster compartidos? ". Todos los puertos también pueden utilizarse como puertos de clúster dedicados.
Reducida	Todos los puertos configurados para conexiones de almacenamiento NVMe de 100 GbE.

Versiones actuales de la secuencia de comandos RCF

Hay dos scripts de RCF disponibles para las aplicaciones de clúster y almacenamiento. Descargar RCFs de "[Descarga del software NVIDIA SN2100](#)" la página. El procedimiento para cada uno es el mismo.

- Cluster: **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**
- Almacenamiento: **MSN2100-RCF-v1.x-Almacenamiento**

Acerca de los ejemplos

El siguiente procedimiento de ejemplo muestra cómo descargar y aplicar el script RCF para los switches de clúster.

El resultado de ejemplo de comando utiliza la dirección IP de gestión del switch 10.233.204.71, la máscara de red 255.255.254.0 y la pasarela predeterminada 10.233.204.1.

Ejemplo 4. Pasos

Cumulus Linux 4.4.3

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el `ping` Comando para verificar la conectividad con el servidor que aloja Cumulus Linux y el RCF.
3. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```

4. 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
```

- b. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

```
network interface show -role cluster
```

- c. Compruebe que el clúster muestra información de ambos switches de clúster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

- Si está actualizando su RCF, debe deshabilitar la reversión automática para este paso.
- Si acaba de actualizar su versión de Cumulus Linux, no necesita deshabilitar la reversión automática para este paso porque ya está deshabilitada.

1. Mostrar las interfaces disponibles en el interruptor SN2100:

```
admin@sw1:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	---	-----	-----	-----	-----
-----	-----	---	-----	-----	-----	-----
...						
...						
ADMDN	swp1	N/A	9216	NotConfigured		
ADMDN	swp2	N/A	9216	NotConfigured		
ADMDN	swp3	N/A	9216	NotConfigured		
ADMDN	swp4	N/A	9216	NotConfigured		
ADMDN	swp5	N/A	9216	NotConfigured		
ADMDN	swp6	N/A	9216	NotConfigured		
ADMDN	swp7	N/A	9216	NotConfigured		
ADMDN	swp8	N/A	9216	NotConfigured		
ADMDN	swp9	N/A	9216	NotConfigured		
ADMDN	swp10	N/A	9216	NotConfigured		
ADMDN	swp11	N/A	9216	NotConfigured		
ADMDN	swp12	N/A	9216	NotConfigured		
ADMDN	swp13	N/A	9216	NotConfigured		
ADMDN	swp14	N/A	9216	NotConfigured		
ADMDN	swp15	N/A	9216	NotConfigured		
ADMDN	swp16	N/A	9216	NotConfigured		

2. Copie la secuencia de comandos de la pitón de RCF en el conmutador.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s          00:00
```



Mientras `scp` En el ejemplo se utiliza, puede utilizar su método preferido de transferencia de archivos, por ejemplo, SFTP, HTTPS o FTP.

3. Aplique el script python de RCF **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.


```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

La secuencia de comandos RCF completa los pasos enumerados en el ejemplo anterior.



En el paso 3 **Actualizar el archivo MOTD** anterior, el comando `cat /etc/motd` se ejecuta. Esto le permite verificar el nombre del archivo RCF, la versión de RCF, los puertos que se deben utilizar y otra información importante en el banner de RCF.



Para cualquier problema de script de Python de RCF que no se pueda corregir, póngase en contacto con ["Soporte de NetApp"](#) para obtener ayuda.

4. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.
5. Verificar la configuración tras el reinicio:

```
admin@sw1:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
...						
...						
DN	swp1s0	N/A	9216	Trunk/L2		Master:
	bridge(UP)					
DN	swp1s1	N/A	9216	Trunk/L2		Master:
	bridge(UP)					
DN	swp1s2	N/A	9216	Trunk/L2		Master:
	bridge(UP)					
DN	swp1s3	N/A	9216	Trunk/L2		Master:

```

bridge (UP)
DN      swp2s0      N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp2s1      N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp2s2      N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp2s3      N/A      9216      Trunk/L2      Master:
bridge (UP)
UP      swp3        100G    9216      Trunk/L2      Master:
bridge (UP)
UP      swp4        100G    9216      Trunk/L2      Master:
bridge (UP)
DN      swp5        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp6        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp7        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp8        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp9        N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp10       N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp11       N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp12       N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp13       N/A      9216      Trunk/L2      Master:
bridge (UP)
DN      swp14       N/A      9216      Trunk/L2      Master:
bridge (UP)
UP      swp15       N/A      9216      BondMember    Master:
bond_15_16 (UP)
UP      swp16       N/A      9216      BondMember    Master:
bond_15_16 (UP)
...
...

```

```

admin@sw1:mgmt:~$ net show roce config

```

```

RoCE mode..... lossless

```

```

Congestion Control:

```

```

    Enabled SPs.... 0 2 5

```

```

    Mode..... ECN

```

```

    Min Threshold.. 150 KB

```

```

Max Threshold.. 1500 KB
PFC:
  Status..... enabled
  Enabled SPs.... 2 5
  Interfaces..... swp10-16,swp1s0-3,swp2s0-3,swp3-9

```

DSCP	802.1p	switch-priority
0 1 2 3 4 5 6 7	0	0
8 9 10 11 12 13 14 15	1	1
16 17 18 19 20 21 22 23	2	2
24 25 26 27 28 29 30 31	3	3
32 33 34 35 36 37 38 39	4	4
40 41 42 43 44 45 46 47	5	5
48 49 50 51 52 53 54 55	6	6
56 57 58 59 60 61 62 63	7	7

switch-priority	TC	ETS
0 1 3 4 6 7	0	DWRR 28%
2	2	DWRR 28%
5	5	DWRR 43%

6. Verifique la información del transceptor en la interfaz:

```

admin@sw1:mgmt:~$ net show interface pluggables
Interface  Identifier      Vendor Name  Vendor PN      Vendor SN
Vendor Rev
-----
swp3       0x11 (QSFP28)  Amphenol    112-00574
APF20379253516 B0
swp4       0x11 (QSFP28)  AVAGO       332-00440      AF1815GU05Z
A0
swp15      0x11 (QSFP28)  Amphenol    112-00573
APF21109348001 B0
swp16      0x11 (QSFP28)  Amphenol    112-00573
APF21109347895 B0

```

7. Compruebe que cada nodo tenga una conexión con cada switch:

```
admin@sw1:mgmt:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	sw1	e3a
swp4	100G	Trunk/L2	sw2	e3b
swp15	100G	BondMember	sw13	swp15
swp16	100G	BondMember	sw14	swp16

8. 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:

```
cluster1::*> network port show -role cluster
```

Node: node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

b. Compruebe el estado del switch del clúster (es posible que esto no muestre el switch sw2, ya que las LIF no son homed en el e0d).

```

cluster1::*> network device-discovery show -protocol lldp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface Platform
-----
node1/lldp
          e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
          e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
          e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
          e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -

cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
-----
sw1                                         cluster-network      10.233.205.90
MSN2100-CB2RC
    Serial Number: MNXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                                Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                                         cluster-network      10.233.205.91
MSN2100-CB2RC
    Serial Number: MNCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                                Technologies Ltd. MSN2100
    Version Source: LLDP

```

9. Compruebe que el clúster esté en buen estado:

```
cluster show
```

10. Repita los pasos 1 a 14 en el segundo interruptor.

11. Habilite la reversión automática en las LIF del clúster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el `ping` Comando para verificar la conectividad con el servidor que aloja Cumulus Linux y el RCF.
3. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```

4. 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
```

- b. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

```
network interface show -role cluster
```

- c. Compruebe que el clúster muestra información de ambos switches de clúster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

- Si está actualizando su RCF, debe deshabilitar la reversión automática para este paso.
- Si acaba de actualizar su versión de Cumulus Linux, no necesita deshabilitar la reversión automática para este paso porque ya está deshabilitada.

1. Mostrar las interfaces disponibles en el interruptor SN2100:

```
admin@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----
+ cluster_isl  9216   200G   up
bond
+ eth0          1500   100M   up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo            65536          up
loopback      IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0        9216   10G    up    cluster01         e0b
swp
.
.
.
+ swp15         9216   100G    up    sw2                swp15
swp
+ swp16         9216   100G    up    sw2                swp16
swp
```

2. Copie la secuencia de comandos de la pitón de RCF en el conmutador.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s          00:00
```



Mientras scp En el ejemplo se utiliza, puede utilizar su método preferido de transferencia de archivos, por ejemplo, SFTP, HTTPS o FTP.

3. Aplique el script python de RCF **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
.
.
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

La secuencia de comandos RCF completa los pasos enumerados en el ejemplo anterior.



En el paso 3 **Actualización del archivo MOTD** anterior, el comando `cat /etc/issue.net` se ejecuta. Esto le permite verificar el nombre del archivo RCF, la versión de RCF, los puertos que se deben utilizar y otra información importante en el banner de RCF.

Por ejemplo:


```

admin@sw1:mgmt:~$ cat /etc/issue.net
*****
*****
*
* NetApp Reference Configuration File (RCF)
* Switch      : Mellanox MSN2100
* Filename     : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version      : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1       : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2       : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14   : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16  : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
*****
*****

```



Para cualquier problema de script de Python de RCF que no se pueda corregir, póngase en contacto con ["Soporte de NetApp"](#) para obtener ayuda.

4. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.
5. Verificar la configuración tras el reinicio:

```

admin@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type           Summary
-----

```

```

+ cluster_isl 9216 200G up
bond
+ eth0          1500 100M up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
    eth0
IP Address: fd20:8ble:f6ff:fe31:4a0e/64
+ lo            65536          up
loopback      IP Address: 127.0.0.1/8
    lo
IP Address: ::1/128
+ swp1s0        9216 10G      up cluster01          e0b
swp
.
.
.
+ swp15         9216 100G      up sw2                  swp15
swp
+ swp16         9216 100G      up sw2                  swp16
swp

admin@sw1:mgmt:~$ nv show qos roce
                        operational  applied  description
-----
enable                  on          Turn feature 'on' or
'off'. This feature is disabled by default.
mode                    lossless   lossless  Roce Mode
congestion-control
    congestion-mode      ECN,RED    Congestion config mode
    enabled-tc           0,2,5     Congestion config enabled
Traffic Class
    max-threshold        195.31 KB Congestion config max-
threshold
    min-threshold        39.06 KB  Congestion config min-
threshold
    probability          100
lldp-app-tlv
    priority             3         switch-priority of roce
    protocol-id          4791      L4 port number
    selector             UDP         L4 protocol
pfc
    pfc-priority         2, 5      switch-prio on which PFC
is enabled
    rx-enabled           enabled    PFC Rx Enabled status
    tx-enabled           enabled    PFC Tx Enabled status
trust

```

trust-mode pcp,dscp Trust Setting on the port
for packet classification

RoCE PCP/DSCP->SP mapping configurations

=====			
--	pcp	dscp	switch-prio

0	0	0,1,2,3,4,5,6,7	0
1	1	8,9,10,11,12,13,14,15	1
2	2	16,17,18,19,20,21,22,23	2
3	3	24,25,26,27,28,29,30,31	3
4	4	32,33,34,35,36,37,38,39	4
5	5	40,41,42,43,44,45,46,47	5
6	6	48,49,50,51,52,53,54,55	6
7	7	56,57,58,59,60,61,62,63	7

RoCE SP->TC mapping and ETS configurations

=====			
--	switch-prio	traffic-class	scheduler-weight

0	0	0	DWRR-28%
1	1	0	DWRR-28%
2	2	2	DWRR-28%
3	3	0	DWRR-28%
4	4	0	DWRR-28%
5	5	5	DWRR-43%
6	6	0	DWRR-28%
7	7	0	DWRR-28%

RoCE pool config

=====					
	name	mode	size	switch-priorities	
traffic-class					
--	-----	-----	----	-----	

0	lossy-default-ingress	Dynamic	50%	0,1,3,4,6,7	-
1	roce-reserved-ingress	Dynamic	50%	2,5	-
2	lossy-default-egress	Dynamic	50%	-	0
3	roce-reserved-egress	Dynamic	inf	-	2,5

Exception List

=====	
--	description

---	...

```

1  RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
2  Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
3  Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
4  Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
5  Congestion Config max-threshold Mismatch.Expected max-
threshold:
    1500000.
6  Scheduler config mismatch for traffic-class mapped to
switch-prio0.
    Expected scheduler-weight: DWRR-50%.
7  Scheduler config mismatch for traffic-class mapped to
switch-prio1.
    Expected scheduler-weight: DWRR-50%.
8  Scheduler config mismatch for traffic-class mapped to
switch-prio2.
    Expected scheduler-weight: DWRR-50%.
9  Scheduler config mismatch for traffic-class mapped to
switch-prio3.
    Expected scheduler-weight: DWRR-50%.
10 Scheduler config mismatch for traffic-class mapped to
switch-prio4.
    Expected scheduler-weight: DWRR-50%.
11 Scheduler config mismatch for traffic-class mapped to
switch-prio5.
    Expected scheduler-weight: DWRR-50%.
12 Scheduler config mismatch for traffic-class mapped to
switch-prio6.
    Expected scheduler-weight: strict-priority.
13 Scheduler config mismatch for traffic-class mapped to
switch-prio7.
    Expected scheduler-weight: DWRR-50%.
14 Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
15 Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
16 Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
17 Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
18 Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
19 Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link

```

fast-linkup

Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link fast-linkup



Las excepciones enumeradas no afectan al rendimiento y se pueden ignorar de forma segura.

6. Verifique la información del transceptor en la interfaz:

```
admin@sw1:mgmt:~$ nv show interface --view=pluggables
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor
SN	Vendor Rev			
-----	-----	-----	-----	
swp1s0	0x00 None			
swp1s1	0x00 None			
swp1s2	0x00 None			
swp1s3	0x00 None			
swp2s0	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s1	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s2	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s3	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp3	0x00 None			
swp4	0x00 None			
swp5	0x00 None			
swp6	0x00 None			
.				
.				
.				
swp15	0x11 (QSFP28)	Amphenol	112-00595	
APF20279210117	B0			
swp16	0x11 (QSFP28)	Amphenol	112-00595	
APF20279210166	B0			

7. Compruebe que cada nodo tenga una conexión con cada switch:

```
admin@sw1:mgmt:~$ nv show interface --view=lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
eth0	100M	Mgmt	mgmt-sw1	Eth110/1/29
swp2s1	25G	Trunk/L2	node1	e0a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

8. 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:

```
cluster1::*> network port show -role cluster
```

Node: node1

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

b. Compruebe el estado del switch del clúster (es posible que esto no muestre el switch sw2, ya que las LIF no son homed en el e0d).

```

cluster1::*> network device-discovery show -protocol lldp
Node/          Local  Discovered
Protocol       Port   Device (LLDP: ChassisID)  Interface Platform
-----
node1/lldp
              e3a    sw1  (b8:ce:f6:19:1a:7e)    swp3      -
              e3b    sw2  (b8:ce:f6:19:1b:96)    swp3      -

node2/lldp
              e3a    sw1  (b8:ce:f6:19:1a:7e)    swp4      -
              e3b    sw2  (b8:ce:f6:19:1b:96)    swp4      -

cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
-----
sw1                                         cluster-network      10.233.205.90
MSN2100-CB2RC
    Serial Number: MNXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                                Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                                         cluster-network      10.233.205.91
MSN2100-CB2RC
    Serial Number: MNCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                                Technologies Ltd. MSN2100
    Version Source: LLDP

```

9. Compruebe que el clúster esté en buen estado:

```
cluster show
```

10. Repita los pasos 1 a 14 en el segundo interruptor.

11. Habilite la reversión automática en las LIF del clúster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el `ping` Comando para verificar la conectividad con el servidor que aloja Cumulus Linux y el RCF.
3. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```

4. 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
```

- b. Compruebe que todas las interfaces del clúster (LIF) están en el puerto de inicio:

```
network interface show -role cluster
```

- c. Compruebe que el clúster muestra información de ambos switches de clúster:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

- Si está actualizando su RCF, debe deshabilitar la reversión automática para este paso.
- Si acaba de actualizar su versión de Cumulus Linux, no necesita deshabilitar la reversión automática para este paso porque ya está deshabilitada.

1. Mostrar las interfaces disponibles en el interruptor SN2100:

```
admin@sw1:mgmt:~$ nv show interface
Interface      MTU    Speed State Remote Host      Remote Port-
Type          Summary
-----
+ cluster_isl  9216   200G   up
bond
+ eth0          1500   100M   up    mgmt-sw1          Eth105/1/14
eth           IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo            65536          up
loopback     IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0        9216   10G    up    cluster01         e0b
swp
.
.
.
+ swp15         9216   100G    up    sw2                swp15
swp
+ swp16         9216   100G    up    sw2                swp16
swp
```

2. Copie la secuencia de comandos de la pitón de RCF en el conmutador.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s          00:00
```



A pesar de scp En el ejemplo se utiliza, puede utilizar su método preferido de transferencia de archivos, por ejemplo, SFTP, HTTPS o FTP.

3. Aplique el script python de RCF **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
.
.
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

La secuencia de comandos RCF completa los pasos enumerados en el ejemplo anterior.



En el paso 3 **Actualización del archivo MOTD** anterior, se ejecuta el comando `cat /etc/issue.net`. Esto le permite verificar el nombre del archivo RCF, la versión de RCF, los puertos que se deben utilizar y otra información importante en el banner de RCF.

Por ejemplo:

```

admin@sw1:mgmt:~$ cat /etc/issue.net
*****
*****
*
* NetApp Reference Configuration File (RCF)
* Switch      : Mellanox MSN2100
* Filename     : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version      : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1       : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2       : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14   : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16  : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
*****
*****

```



Para cualquier problema de script de Python de RCF que no se pueda corregir, póngase en contacto con ["Soporte de NetApp"](#) para obtener ayuda.

4. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.
5. Verificar la configuración tras el reinicio:

```

admin@sw1:mgmt:~$ nv show interface
Interface      MTU   Speed State Remote Host      Remote Port-
Type           Summary
-----
-----

```

```

+ cluster_isl 9216 200G up
bond
+ eth0          1500 100M up    mgmt-sw1          Eth105/1/14
eth            IP Address: 10.231.80 206/22
    eth0
IP Address: fd20:8ble:f6ff:fe31:4a0e/64
+ lo            65536          up
loopback      IP Address: 127.0.0.1/8
    lo
IP Address: ::1/128
+ swp1s0        9216 10G      up cluster01          e0b
swp
.
.
.
+ swp15         9216 100G      up sw2              swp15
swp
+ swp16         9216 100G      up sw2              swp16
swp

admin@sw1:mgmt:~$ nv show qos roce
                    operational  applied  description
-----
enable              on          Turn feature 'on' or
'off'. This feature is disabled by default.
mode                lossless   lossless  Roce Mode
congestion-control
  congestion-mode    ECN,RED    Congestion config mode
  enabled-tc         0,2,5     Congestion config enabled
Traffic Class
  max-threshold      195.31 KB Congestion config max-
threshold
  min-threshold      39.06 KB  Congestion config min-
threshold
  probability        100
lldp-app-tlv
  priority           3          switch-priority of roce
  protocol-id        4791       L4 port number
  selector           UDP        L4 protocol
pfc
  pfc-priority       2, 5       switch-prio on which PFC
is enabled
  rx-enabled         enabled    PFC Rx Enabled status
  tx-enabled         enabled    PFC Tx Enabled status
trust

```

trust-mode pcp,dscp Trust Setting on the port
for packet classification

RoCE PCP/DSCP->SP mapping configurations

=====			
--	pcp	dscp	switch-prio
---	-----	-----	-----
0	0	0,1,2,3,4,5,6,7	0
1	1	8,9,10,11,12,13,14,15	1
2	2	16,17,18,19,20,21,22,23	2
3	3	24,25,26,27,28,29,30,31	3
4	4	32,33,34,35,36,37,38,39	4
5	5	40,41,42,43,44,45,46,47	5
6	6	48,49,50,51,52,53,54,55	6
7	7	56,57,58,59,60,61,62,63	7

RoCE SP->TC mapping and ETS configurations

=====			
--	switch-prio	traffic-class	scheduler-weight
---	-----	-----	-----
0	0	0	DWRR-28%
1	1	0	DWRR-28%
2	2	2	DWRR-28%
3	3	0	DWRR-28%
4	4	0	DWRR-28%
5	5	5	DWRR-43%
6	6	0	DWRR-28%
7	7	0	DWRR-28%

RoCE pool config

=====					
	name	mode	size	switch-priorities	
traffic-class					
--	-----	-----	----	-----	

0	lossy-default-ingress	Dynamic	50%	0,1,3,4,6,7	-
1	roce-reserved-ingress	Dynamic	50%	2,5	-
2	lossy-default-egress	Dynamic	50%	-	0
3	roce-reserved-egress	Dynamic	inf	-	2,5

Exception List

=====	
--	description

---	...

```

1  RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
2  Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
3  Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
4  Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
5  Congestion Config max-threshold Mismatch.Expected max-
threshold:
    1500000.
6  Scheduler config mismatch for traffic-class mapped to
switch-prio0.
    Expected scheduler-weight: DWRR-50%.
7  Scheduler config mismatch for traffic-class mapped to
switch-prio1.
    Expected scheduler-weight: DWRR-50%.
8  Scheduler config mismatch for traffic-class mapped to
switch-prio2.
    Expected scheduler-weight: DWRR-50%.
9  Scheduler config mismatch for traffic-class mapped to
switch-prio3.
    Expected scheduler-weight: DWRR-50%.
10 Scheduler config mismatch for traffic-class mapped to
switch-prio4.
    Expected scheduler-weight: DWRR-50%.
11 Scheduler config mismatch for traffic-class mapped to
switch-prio5.
    Expected scheduler-weight: DWRR-50%.
12 Scheduler config mismatch for traffic-class mapped to
switch-prio6.
    Expected scheduler-weight: strict-priority.
13 Scheduler config mismatch for traffic-class mapped to
switch-prio7.
    Expected scheduler-weight: DWRR-50%.
14 Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
15 Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
16 Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
17 Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
18 Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
19 Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link

```

```
fast-linkup
```

```
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```



Las excepciones enumeradas no afectan al rendimiento y se pueden ignorar de forma segura.

6. Verifique la información del transceptor en la interfaz:

```
admin@sw1:mgmt:~$ nv show platform transceiver
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor
SN	Vendor Rev			
-----	-----	-----	-----	
swp1s0	0x00 None			
swp1s1	0x00 None			
swp1s2	0x00 None			
swp1s3	0x00 None			
swp2s0	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s1	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s2	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp2s3	0x11 (QSFP28)	CISCO-LEONI	L45593-D278-D20	
LCC2321GTTJ	00			
swp3	0x00 None			
swp4	0x00 None			
swp5	0x00 None			
swp6	0x00 None			
.				
.				
.				
swp15	0x11 (QSFP28)	Amphenol	112-00595	
APF20279210117	B0			
swp16	0x11 (QSFP28)	Amphenol	112-00595	
APF20279210166	B0			

7. Compruebe que cada nodo tenga una conexión con cada switch:

```
admin@sw1:mgmt:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
eth0	100M	Mgmt	mgmt-sw1	Eth110/1/29
swp2s1	25G	Trunk/L2	node1	e0a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

8. 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:

```
cluster1::*> network port show -role cluster
```

Node: node1

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
e3a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/10000

b. Compruebe el estado del switch del clúster (es posible que esto no muestre el switch sw2, ya que las LIF no son homed en el e0d).


```

cluster1::*> network device-discovery show -protocol lldp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface Platform
-----
node1/lldp
          e3a    sw1 (b8:ce:f6:19:1a:7e)  swp3      -
          e3b    sw2 (b8:ce:f6:19:1b:96)  swp3      -

node2/lldp
          e3a    sw1 (b8:ce:f6:19:1a:7e)  swp4      -
          e3b    sw2 (b8:ce:f6:19:1b:96)  swp4      -

cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch              Type              Address
Model
-----
-----
sw1                  cluster-network    10.233.205.90
MSN2100-CB2RC
    Serial Number: MNXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                  cluster-network    10.233.205.91
MSN2100-CB2RC
    Serial Number: MNCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

```

9. Compruebe que el clúster esté en buen estado:

```
cluster show
```

10. Repita los pasos 1 a 14 en el segundo interruptor.

11. Habilite la reversión automática en las LIF del clúster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

El futuro

"Instale el archivo CSHM".

Instale el archivo de configuración del monitor de estado del switch Ethernet

Para configurar la supervisión del estado del conmutador Ethernet en los conmutadores Ethernet NVIDIA, siga este procedimiento.

Estas instrucciones se aplican si los conmutadores NVIDIA X190006-PE y X190006-PI no se detectan correctamente, lo que se puede confirmar ejecutando `system switch ethernet show` y comprobar si se muestra **OTRO** para su modelo. Para identificar el modelo de su conmutador NVIDIA, busque el número de pieza con el comando `nv show platform hardware` para NVIDIA CL 5.8 y anteriores o `nv show platform` para versiones posteriores.



Estos pasos también se recomiendan si desea que la monitorización del estado y la recopilación de registros funcionen correctamente al usar NVIDIA CL 5.11.x con las siguientes versiones de ONTAP. Si bien la monitorización del estado y la recopilación de registros podrían seguir funcionando sin estos pasos, seguirlos garantiza que todo funcione correctamente.

- 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 y versiones de parches posteriores

Antes de empezar

- Asegúrese de que el clúster de ONTAP esté en funcionamiento.
- Habilite SSH en el conmutador para utilizar todas las funciones disponibles en CSHM.
- Borre el `/mroot/etc/cshm_nod/nod_sign/` directorio en todos los nodos:

- a. Entra en el infierno:

```
system node run -node <name>
```

- b. Cambiar a privilegio avanzado:

```
priv set advanced
```

- c. Enumere los archivos de configuración en el `/etc/cshm_nod/nod_sign` directorio. Si el directorio existe y contiene archivos de configuración, enumera los nombres de archivo.

```
ls /etc/cshm_nod/nod_sign
```

- d. Elimine todos los archivos de configuración correspondientes a los modelos de switch conectados.

Si no está seguro, elimine todos los archivos de configuración de los modelos compatibles enumerados anteriormente y, a continuación, descargue e instale los archivos de configuración más recientes para esos mismos modelos.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

- a. Confirme que los archivos de configuración eliminados ya no están en el directorio:

```
ls /etc/cshm_nod/nod_sign
```

Pasos

1. Descargue el archivo zip de configuración del monitor de estado del switch Ethernet según la versión de ONTAP correspondiente. Este archivo está disponible en la ["Switches Ethernet de NVIDIA"](#) página.
 - a. En la página de descarga del software NVIDIA SN2100, seleccione **Nvidia CSHM File**.
 - b. En la página Precaución/debe leer, seleccione la casilla de verificación para aceptar.
 - c. En la página Contrato de licencia de usuario final, seleccione la casilla de verificación para aceptar y haga clic en **Aceptar y continuar**.
 - d. En la página Nvidia CSHM File - Download, seleccione el archivo de configuración aplicable. Están disponibles los siguientes archivos:

ONTAP 9.15.1 y versiones posteriores

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 a 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. Cargue el archivo zip correspondiente al servidor web interno.
2. Acceda a la configuración de modo avanzado desde uno de los sistemas ONTAP en el clúster.

```
set -privilege advanced
```

3. Ejecute el comando switch health monitor configure.

```
cluster1::> system switch ethernet
```

4. Compruebe que el resultado del comando termine con el siguiente texto para su versión de ONTAP:

ONTAP 9.15.1 y versiones posteriores

La supervisión de estado del switch Ethernet ha instalado el archivo de configuración.

ONTAP 9.11.1 a 9.14.1

SHM instaló el archivo de configuración.

ONTAP 9.10.1

El paquete descargado de CSHM se ha procesado correctamente.

Si se produce un error, póngase en contacto con el soporte de NetApp.

1. Espere hasta dos veces el intervalo de sondeo del monitor de estado del switch Ethernet, que se encuentra ejecutando `system switch ethernet polling-interval show`, antes de completar el siguiente paso.
2. Ejecute el comando `system switch ethernet show` en el sistema ONTAP y asegúrese de que los conmutadores del clúster se descubran con el campo Monitorizado establecido en **Verdadero** y el campo de número de serie no muestre **Desconocido**.

```
cluster1::> system switch ethernet show
```



Si su modelo sigue mostrando **OTHER** después de aplicar el archivo de configuración, póngase en contacto con el servicio de asistencia técnica de NetApp.

Ver el "[Monitor de estado de configuración Ethernet del conmutador del sistema](#)" Comando para más detalles.

El futuro

["Configure la supervisión de estado del switch"](#).

Restablecer el interruptor del clúster SN2100 a los valores predeterminados de fábrica

Para restablecer el interruptor del clúster SN2100 a los valores predeterminados de fábrica:

- Para Cumulus Linux 5.10 y versiones anteriores, aplique la imagen de Cumulus.
- Para Cumulus Linux 5.11 y posteriores, utilice el `nv action reset system factory-default dominio`.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Debe tener la contraseña root para acceder a los comandos de sudo.



Para obtener más información sobre la instalación de Cumulus Linux, consulte "[Flujo de trabajo de instalación de software para los switches NVIDIA SN2100](#)".

Ejemplo 5. Pasos

Cumulus Linux 5.10 y anteriores

1. Desde la consola Cumulus, descargue y ponga en cola la instalación del software del conmutador con el comando `onie-install -a -i` Seguido de la ruta del archivo al software del conmutador, por ejemplo:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. El instalador inicia la descarga. Escriba **y** cuando se le solicite para confirmar la instalación cuando se haya descargado y verificado la imagen.
3. Reinicie el conmutador para instalar el nuevo software.

```
sudo reboot
```

```
cumulus@sw1:mgmt:~$ sudo reboot
```



El conmutador se reinicia y accede a la instalación del software del conmutador, lo que lleva algún tiempo. Cuando se completa la instalación, el conmutador se reinicia y permanece en el log-in inmediato.

Cumulus Linux 5.11 y posteriores

1. Para restablecer el interruptor a los valores predeterminados de fábrica y eliminar toda la configuración, los archivos del sistema y los archivos de registro, ejecute:

```
nv action reset system factory-default
```

Por ejemplo:

```
cumulus@switch:~$ nv action reset system factory-default
```

```
This operation will reset the system configuration, delete the log files and reboot the switch.
```

```
Type [y] continue.
```

```
Type [n] to abort.
```

```
Do you want to continue? [y/n] y
```

Ver NVIDIA ["Restablecimiento de fábrica"](#) documentación para más detalles.

Migrar los switches

Migre switches de clúster CN1610 a switches de clúster NVIDIA SN2100

Los switches de clúster CN1610 de NetApp se pueden migrar para un clúster de ONTAP a los switches de clúster de NVIDIA SN2100. Se trata de un procedimiento no disruptivo.

Revise los requisitos

Debe estar al tanto de cierta información de configuración, conexiones de puertos y requisitos de cableado cuando se reemplazan los switches de clúster NetApp CN1610 por switches de clústeres NVIDIA SN2100. Consulte ["Descripción general de la instalación y configuración de los switches NVIDIA SN2100"](#).

Switches compatibles

Se admiten los siguientes switches de clúster:

- CN1610 de NetApp
- NVIDIA SN2100

Para obtener más información acerca de los puertos admitidos y sus configuraciones, consulte ["Hardware Universe"](#).

Antes de empezar

Compruebe que cumple los siguientes requisitos para la configuración:

- El clúster existente está correctamente configurado y funcionando.
- Todos los puertos de clúster se encuentran en el estado **up** para garantizar operaciones no disruptivas.
- Los switches de clúster NVIDIA SN2100 se configuran y funcionan con la versión correcta de Cumulus Linux instalada con el archivo de configuración de referencia (RCF) aplicado.
- La configuración de red del clúster existente tiene lo siguiente:
 - Un clúster de NetApp redundante y completamente funcional que utiliza switches CN1610.
 - La conectividad de gestión y el acceso a la consola tanto a los switches CN1610 como a los nuevos.
 - Todas las LIF de clúster están en estado activo con las LIF de clúster en sus puertos iniciales.
 - Puertos ISL habilitados y cableados entre los switches CN1610 y entre los nuevos switches.
- Algunos puertos están configurados en los switches NVIDIA SN2100 para funcionar a 40GbE o 100GbE Gbps.
- Ha planificado, migrado y documentado conectividad 40GbE y 100GbE desde los nodos a los switches de clúster NVIDIA SN2100.

Migrar los switches

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los switches de clúster CN1610 existentes son *C1* y *C2*.
- Los nuevos switches de clúster NVIDIA SN2100 son *sw1* y *sw2*.
- 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.
- La `cluster1::*>` prompt indica el nombre del clúster.

- Los puertos de clúster utilizados en este procedimiento son *e3a* y *e3b*.
- Los puertos de arranque tienen el formato: *swp[Port][breakout Port 0-3]*. Por ejemplo, cuatro puertos de arranque en *swp1* son *swp1s0*, *swp1s1*, *swp1s2* y *swp1s3*.

Acerca de esta tarea

Este procedimiento cubre el siguiente caso:

- El interruptor C2 se reemplaza primero por el interruptor SW2.
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - Después, el cableado entre los nodos y C2 se desconecta del C2 y se vuelve a conectar al SW2.
- El interruptor C1 se reemplaza por el interruptor sw1.
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - Después, el cableado entre los nodos y C1 se desconecta del C1 y se vuelve a conectar al sw1.



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.

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
```

donde *x* es la duración de la ventana de mantenimiento en horas.

2. Cambie el nivel de privilegio a avanzado, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

3. Deshabilite la reversión automática en las LIF del clúster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

Paso 2: Configure los puertos y el cableado

1. Determinar el estado administrativo u operativo de cada interfaz de clúster.

Cada puerto debería mostrarse para *Link y.. healthy* 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
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
-----	-----				
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

b. Muestre información sobre las LIF y sus nodos iniciales designados:

```
network interface show -vserver Cluster
```

Cada LIF debería mostrar up/up para Status Admin/Oper y.. true para Is Home.

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				
e3a	node1_clus1	up/up	169.254.209.69/16	node1
e3b	true			
e3a	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true			
e3a	node2_clus1	up/up	169.254.47.194/16	node2
e3b	true			
e3a	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true			

- Los puertos de 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
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

node1	/cdp			
	e3a	c1 (6a:ad:4f:98:3b:3f)	0/1	-
	e3b	c2 (6a:ad:4f:98:4c:a4)	0/1	-
node2	/cdp			
	e3a	c1 (6a:ad:4f:98:3b:3f)	0/2	-
	e3b	c2 (6a:ad:4f:98:4c:a4)	0/2	-

- Los puertos y los switches del clúster se conectan 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 e3a	0/1	124	H	AFF-A400
node2 e3a	0/2	124	H	AFF-A400
c2 0/13	0/13	179	S I s	CN1610
c2 0/14	0/14	175	S I s	CN1610
c2 0/15	0/15	179	S I s	CN1610
c2 0/16	0/16	175	S I s	CN1610

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 e3b	0/1	124	H	AFF-A400
node2 e3b	0/2	124	H	AFF-A400
c1 0/13	0/13	175	S I s	CN1610
c1 0/14	0/14	175	S I s	CN1610
c1 0/15	0/15	175	S I s	CN1610
c1 0/16	0/16	175	S I s	CN1610

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					

node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e3a
Cluster node1_clus2 169.254.49.125 node1      e3b
Cluster node2_clus1 169.254.47.194 node2      e3a
Cluster node2_clus2 169.254.19.183 node2      e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:.....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. En el switch C2, apague los puertos conectados a los puertos de cluster de los nodos para conmutar las LIF de cluster.

```

(c2)# configure
(c2)(Config)# interface 0/1-0/12
(c2)(Interface 0/1-0/12)# shutdown
(c2)(Interface 0/1-0/12)# exit
(c2)(Config)# exit
(c2)#

```

2. Mueva los puertos del clúster de nodos desde el conmutador c2 antiguo al nuevo conmutador sw2, utilizando el cableado apropiado que admite NVIDIA SN2100.
3. Mostrar los atributos del puerto de red:

```

network port show -ipspace Cluster

```

Muestra el ejemplo

```
cluster1::*> network port show -ipspace Cluster
```

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

4. 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
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/	Local	Discovered			
Protocol	Port	Device	(LLDP: ChassisID)	Interface	
Platform					

node1	/lldp				
	e3a	c1	(6a:ad:4f:98:3b:3f)	0/1	-
	e3b	sw2	(b8:ce:f6:19:1a:7e)	swp3	-
node2	/lldp				
	e3a	c1	(6a:ad:4f:98:3b:3f)	0/2	-
	e3b	sw2	(b8:ce:f6:19:1b:96)	swp4	-

5. En el switch sw2, compruebe que todos los puertos del clúster de nodos estén activos:

```
net show interface
```

Muestra el ejemplo

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

6. En el switch C1, apague los puertos conectados a los puertos de clúster de los nodos para conmutar las LIF de clúster.


```
(c1)# configure
(c1) (Config)# interface 0/1-0/12
(c1) (Interface 0/1-0/12)# shutdown
(c1) (Interface 0/1-0/12)# exit
(c1) (Config)# exit
(c1)#
```

7. Mueva los puertos del clúster de nodos del conmutador c1 antiguo al conmutador sw1 nuevo, utilizando el cableado adecuado que admite NVIDIA SN2100.
8. Compruebe la configuración final del clúster:

```
network port show -ipspace Cluster
```

Cada puerto debe aparecer up para Link y.. healthy 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							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	----	----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

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
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1	/lldp			
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-
node2	/lldp			
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-

10. En los switches sw1 y sw2, verifique que todos los puertos del clúster de nodos estén activos:

```
net show interface
```

Muestra el ejemplo

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3a
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3a
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw2 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw2 (swp16)
Master: cluster_isl(UP)					

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

11. Compruebe que ambos nodos tengan una conexión cada uno con cada switch:

```
net show lldp
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran los resultados adecuados para ambos switches:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

Paso 3: Verificar la configuración

1. Habilite la reversión automática en las LIF del clúster:

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert  
true
```

2. Compruebe que todos los LIF de red del clúster vuelven a estar en sus puertos raíz:

```
network interface show
```

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
e3a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e3a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true			

3. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

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
```

El futuro

["Configure la supervisión de estado del switch".](#)

Migrar desde un switch de clúster de Cisco a un switch de clúster NVIDIA SN2100

Puede migrar switches de clúster de Cisco para un clúster de ONTAP a switches de clúster NVIDIA SN2100. Se trata de un procedimiento no disruptivo.

Revise los requisitos

Debe conocer determinada información de configuración, las conexiones de puertos y los requisitos de cableado cuando sustituya algunos switches de clúster Cisco anteriores por switches de clúster NVIDIA SN2100. Consulte ["Descripción general de la instalación y configuración de los switches NVIDIA SN2100"](#).

Switches compatibles

Se admiten los siguientes switches de clúster de Cisco:

- Nexus 9336C-FX2

- Nexus 92300YC
- Nexus 5596UP
- Nexus 3232C
- Nexus 3132Q-V

Para obtener más información acerca de los puertos admitidos y sus configuraciones, consulte ["Hardware Universe"](#) .

Lo que necesitará

Asegúrese de que:

- El clúster existente está configurado y funciona correctamente.
- Todos los puertos de clúster se encuentran en el estado **up** para garantizar operaciones no disruptivas.
- Los conmutadores de clúster NVIDIA SN2100 están configurados y funcionan con la versión adecuada de Cumulus Linux instalada con el archivo de configuración de referencia (RCF) aplicado.
- La configuración de red del clúster existente tiene lo siguiente:
 - 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 en estado activo con las LIF del clúster están en sus puertos iniciales.
 - Puertos ISL habilitados y cableado entre los switches de Cisco anteriores y entre los switches nuevos.
- Algunos puertos se configuran en los switches NVIDIA SN2100 para que se ejecuten a 40 GbE o 100 GbE.
- Ha planificado, migrado y documentado conectividad de 40 GbE y 100 GbE desde los nodos a switches de clúster NVIDIA SN2100.



Si está cambiando la velocidad de puerto de los puertos de los clústeres de e0a y e1a en sistemas AFF A800 o AFF C800, puede observar que se están recibiendo paquetes con formato incorrecto tras la conversión de velocidad. Consulte ["Error 1570339"](#) Y el artículo de la base de conocimientos ["Errores de CRC en puertos T6 después de convertir de 40GbE a 100GbE"](#) para obtener orientación.

Migrar los switches

Acerca de los ejemplos

En este procedimiento, se utilizan switches de clúster Cisco Nexus 3232C para comandos y salidas de ejemplo.

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los switches de clúster existentes de Cisco Nexus 3232C son *c1* y *c2*.
- Los nuevos switches de clúster NVIDIA SN2100 son *sw1* y *sw2*.
- 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.
- La `cluster1::*>` prompt indica el nombre del clúster.
- Los puertos de clúster utilizados en este procedimiento son *e3a* y *e3b*.

- Los puertos de arranque tienen el formato: swp[Port]s[breakout Port 0-3]. Por ejemplo, cuatro puertos de arranque en swp1 son *swp1s0*, *swp1s1*, *swp1s2* y *swp1s3*.

Acerca de esta tarea

Este procedimiento cubre el siguiente caso:

- El interruptor C2 se reemplaza primero por el interruptor SW2.
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - El cableado entre los nodos y c2 se desconecta de c2 y se vuelve a conectar a sw2.
- El interruptor C1 se reemplaza por el interruptor sw1.
 - Apague los puertos de los nodos del clúster. Todos los puertos deben apagarse simultáneamente para evitar la inestabilidad del clúster.
 - El cableado entre los nodos y c1 se desconecta de c1 y se vuelve a conectar a sw1.

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
```

donde x es la duración de la ventana de mantenimiento en horas.

2. Cambie el nivel de privilegio a avanzado, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

3. Deshabilite la reversión automática en las LIF del clúster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

Paso 2: Configure los puertos y el cableado

1. Determinar 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
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node2

Ignore

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	-----	-----
-----	-----				
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

b. Muestra información sobre las interfaces lógicas y sus nodos principales designados:

```
network interface show -vserver Cluster
```

Cada LIF debería mostrar up/up para 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				
e3a	node1_clus1	up/up	169.254.209.69/16	node1
e3b	true			
e3a	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true			
e3a	node2_clus1	up/up	169.254.47.194/16	node2
e3b	true			
e3a	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true			

2. Los puertos de clúster de cada nodo están conectados a los switches de clúster existentes de la siguiente manera (desde la perspectiva de los nodos):

```
network device-discovery show -protocol lldp
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

node1	/lldp			
e3a	c1	(6a:ad:4f:98:3b:3f)	Eth1/1	-
e3b	c2	(6a:ad:4f:98:4c:a4)	Eth1/1	-
node2	/lldp			
e3a	c1	(6a:ad:4f:98:3b:3f)	Eth1/2	-
e3b	c2	(6a:ad:4f:98:4c:a4)	Eth1/2	-

3. Los switches y los puertos de clúster están conectados de la siguiente manera (desde la perspectiva de los switches):

```
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 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
c2 Eth1/31	Eth1/31	179	S I s	N3K-C3232C
c2 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

```
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 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
c1 Eth1/31	Eth1/31	175	S I s	N3K-C3232C
c1 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e3a
Cluster node1_clus2 169.254.49.125 node1      e3b
Cluster node2_clus1 169.254.47.194 node2      e3a
Cluster node2_clus2 169.254.19.183 node2      e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:.....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. En el switch C2, apague los puertos conectados a los puertos de cluster de los nodos para conmutar las LIF de cluster.

```

(c2)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c2) (Config)# interface
(c2) (config-if-range)# shutdown <interface_list>
(c2) (config-if-range)# exit
(c2) (Config)# exit
(c2)#

```

2. Mueva los puertos del clúster de nodos desde el conmutador c2 antiguo al nuevo conmutador sw2, utilizando el cableado apropiado que admite NVIDIA SN2100.
3. Mostrar los atributos del puerto de red:

```

network port show -ipspace Cluster

```

Muestra el ejemplo

```
cluster1::*> network port show -ipspace Cluster
```

Node: node1

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

4. Los puertos de clúster de cada nodo ahora están conectados a los switches de clúster del siguiente modo, desde la perspectiva de los nodos:

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/	Local	Discovered		
Protocol	Port	Device	(LLDP: ChassisID)	Interface
Platform				
-----	-----	-----	-----	-----
node1	/lldp			
	e3a	c1	(6a:ad:4f:98:3b:3f)	Eth1/1 -
	e3b	sw2	(b8:ce:f6:19:1a:7e)	swp3 -
node2	/lldp			
	e3a	c1	(6a:ad:4f:98:3b:3f)	Eth1/2 -
	e3b	sw2	(b8:ce:f6:19:1b:96)	swp4 -

5. En el switch sw2, compruebe que todos los puertos del clúster de nodos estén activos:

```
net show interface
```

Muestra el ejemplo

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					
-----	-----	-----	-----	-----	-----
...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

6. En el switch C1, apague los puertos conectados a los puertos de clúster de los nodos para conmutar las LIF de clúster.

```
(c1)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c1) (Config)# interface
(c1) (config-if-range)# shutdown <interface_list>
(c1) (config-if-range)# exit
(c1) (Config)# exit
(c1)#
```

7. Mueva los puertos del clúster de nodos del conmutador c1 antiguo al conmutador sw1 nuevo, utilizando el cableado adecuado que admite NVIDIA SN2100.
8. Compruebe la configuración final del clúster:

```
network port show -ipSpace Cluster
```

Cada puerto debe aparecer up 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							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

Node: node2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	-----	-----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

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:

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1	/lldp			
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-
node2	/lldp			
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-

10. En los switches sw1 y sw2, verifique que todos los puertos del clúster de nodos estén activos:

```
net show interface
```

Muestra el ejemplo

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3a
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3a
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw2 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw2 (swp16)
Master: cluster_isl(UP)					

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	e3b
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

11. Compruebe que ambos nodos tengan una conexión cada uno con cada switch:

```
net show lldp
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran los resultados adecuados para ambos switches:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

Paso 3: Verificar la configuración

1. Habilite la reversión automática en las LIF del clúster:

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert  
true
```

2. Compruebe que todos los LIF de red del clúster vuelven a estar en sus puertos raíz:

```
network interface show
```

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				
e3a	node1_clus1	up/up	169.254.209.69/16	node1
	true			
e3b	node1_clus2	up/up	169.254.49.125/16	node1
	true			
e3a	node2_clus1	up/up	169.254.47.194/16	node2
	true			
e3b	node2_clus2	up/up	169.254.19.183/16	node2
	true			

3. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

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
```

El futuro

["Configure la supervisión de estado del switch".](#)

Migre a un clúster con switches de dos nodos con switches de clúster NVIDIA SN2100

Si ya dispone de un entorno de clúster sin switches de dos nodos, puede migrar a un entorno de clústeres con switches de dos nodos mediante switches NVIDIA SN2100 para permitir el escalado 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 Twinax, pero no es compatible con este switch si los nodos utilizan puertos RJ45 10GBASE-T integrados para los puertos de red del clúster.

Revise los requisitos

Configuración con dos nodos sin switches

Asegúrese de que:

- La configuración sin switch de dos nodos está correctamente configurada y funciona.
- Los nodos ejecutan ONTAP 9.10.1P3 y una versión posterior.
- 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.

Configuración de switch de clúster NVIDIA SN2100

Asegúrese de que:

- Ambos switches tienen conectividad de red de gestión.
- Hay acceso de la consola a los switches de clúster.
- El switch de nodo a nodo NVIDIA SN2100 y las conexiones de switch a switch utilizan cables Twinax o de fibra.



Consulte "[Revise las consideraciones sobre el cableado y la configuración](#)" para obtener advertencias e información adicional. La "[Hardware Universe - interruptores](#)" también contiene más información sobre el cableado.

- Los cables de enlace entre switches (ISL) están conectados a los puertos swp15 y swp16 en ambos switches NVIDIA SN2100.
- Se ha completado la personalización inicial de los dos conmutadores SN2100, de modo que:
 - Los conmutadores SN2100 ejecutan la última versión de Cumulus Linux
 - Los archivos de configuración de referencia (RCF) se aplican a los conmutadores
 - Cualquier personalización de sitio, como SMTP, SNMP y SSH, se configura en los nuevos switches.

La "[Hardware Universe](#)" contiene la información más reciente acerca de los puertos del clúster reales para las plataformas.

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 interruptores SN2100 son *sw1* y *sw2*.
- 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 *e3a* y *e3b*.
- Los puertos de arranque tienen el formato: `swp[Port]s[breakout Port 0-3]`. Por ejemplo, cuatro puertos de arranque en *swp1* son *swp1s0*, *swp1s1*, *swp1s2* y *swp1s3*.

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`
donde *x* es la duración de la ventana de mantenimiento en horas.

2. Cambie el nivel de privilegio a Advanced, introduzca `y` cuando se le solicite continuar: `set -privilege advanced`

El aviso avanzado (*>) aparece.

Paso 2: Configure los puertos y el cableado

Cumulus Linux 4.4.x

1. Deshabilite todos los puertos orientados al nodo (no los puertos ISL) en los nuevos switches del clúster sw1 y sw2.

No debe deshabilitar los puertos ISL.

Los siguientes comandos desactivan los puertos orientados al nodo en los switches sw1 y sw2:

```
cumulus@sw1:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit

cumulus@sw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

2. Compruebe que el ISL y los puertos físicos del ISL entre los dos switches SN2100 sw1 y sw2 están en los puertos swp15 y swp16:

```
net show interface
```

Los siguientes comandos muestran que los puertos ISL están activos en los switches sw1 y SW2:


```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp15	100G	9216	BondMember	sw2 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	sw2 (swp16)	Master: cluster_isl (UP)

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp15	100G	9216	BondMember	sw1 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	sw1 (swp16)	Master: cluster_isl (UP)

Cumulus Linux 5.x

1. Deshabilite todos los puertos orientados al nodo (no puertos ISL) en los dos switches de clúster nuevos sw1 y SW2.

No debe deshabilitar los puertos ISL.

Los siguientes comandos desactivan los puertos orientados al nodo en los switches sw1 y sw2:

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
down  
cumulus@sw1:~$ nv config apply  
cumulus@sw1:~$ nv config save  
  
cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
down  
cumulus@sw2:~$ nv config apply  
cumulus@sw2:~$ nv config save
```

2. Compruebe que el ISL y los puertos físicos del ISL entre los dos switches SN2100 sw1 y sw2 están en los puertos swp15 y swp16:

```
nv show interface
```

Los ejemplos siguientes muestran que los puertos ISL están activos en los switches sw1 y SW2:

```
cumulus@sw1:~$ nv show interface
```

Interface	MTU	Speed	State	Remote Host	Remote Port
Type	Summary				

...					
...					
+ swp14	9216		down		
swp					
+ swp15	9216	100G	up	oss-g-rcf1	Intra-Cluster Switch
ISL Port swp15 swp					
+ swp16	9216	100G	up	oss-g-rcf2	Intra-Cluster Switch
ISL Port swp16 swp					

```
cumulus@sw2:~$ nv show interface
```

Interface	MTU	Speed	State	Remote Host	Remote Port
Type	Summary				

...					
...					
+ swp14	9216		down		
swp					
+ swp15	9216	100G	up	oss-g-rcf1	Intra-Cluster Switch
ISL Port swp15 swp					
+ swp16	9216	100G	up	oss-g-rcf2	Intra-Cluster Switch
ISL Port swp16 swp					

1. Verifique que todos los puertos del clúster estén activos:

```
network port show
```

Cada puerto debe aparecer up para Link y saludable para Health Status.

Muestra el ejemplo

```
cluster1::*> network port show
```

Node: node1

Ignore

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	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					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

2. Compruebe que todas las LIF del clúster estén en funcionamiento:

```
network interface show
```

Cada LIF de clúster debería mostrar el valor true para Is Home y que tengan un Status Admin/Oper de up/up.

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
e3a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e3a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true			

3. Deshabilite la reversión automática en las LIF del clúster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

Muestra el ejemplo

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert false
```

	Logical	
Vserver	Interface	Auto-revert

Cluster		
	node1_clus1	false
	node1_clus2	false
	node2_clus1	false
	node2_clus2	false

4. Desconecte el cable del puerto del clúster e3a del nodo 1 y, a continuación, conecte e3a al puerto 3 del conmutador del cluster sw1, utilizando el cableado adecuado admitido por los conmutadores SN2100.

La ["Hardware Universe - interruptores"](#) contiene más información sobre el cableado.

5. Desconecte el cable del puerto del clúster e3a en el nodo 2 y, a continuación, conecte e3a al puerto 4 del

interruptor del cluster sw1, utilizando el cableado adecuado admitido por los interruptores SN2100.

Cumulus Linux 4.4.x

1. En el switch sw1, habilite todos los puertos orientados al nodo.

Los siguientes comandos habilitan todos los puertos orientados al nodo del switch sw1.

```
cumulus@sw1:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link  
down  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

2. En el switch sw1, verifique que todos los puertos estén activos:

```
net show interface all
```

```
cumulus@sw1:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
...						
DN	swp1s0	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s1	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s2	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s3	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s0	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s1	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s2	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s3	25G	9216	Trunk/L2		Master:
br_default(UP)						
UP	swp3	100G	9216	Trunk/L2	node1 (e3a)	Master:
br_default(UP)						
UP	swp4	100G	9216	Trunk/L2	node2 (e3a)	Master:
br_default(UP)						
...						
...						
UP	swp15	100G	9216	BondMember	swp15	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	swp16	Master:
cluster_isl(UP)						
...						

Cumulus Linux 5.x

1. En el switch sw1, habilite todos los puertos orientados al nodo.

Los siguientes comandos habilitan todos los puertos orientados al nodo del switch sw1.

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
up
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

2. En el switch sw1, verifique que todos los puertos estén activos:

```
nv show interface
```

```
cumulus@sw1:~$ nv show interface
```

Interface	State	Speed	MTU	Type	Remote Host
Remote Port	Summary				
-----	-----	-----	-----	-----	
-----	-----	-----	-----	-----	-----
...					
...					
swp1s0	up	10G	9216	swp	odq-a300-1a
e0a					
swp1s1	up	10G	9216	swp	odq-a300-1b
e0a					
swp1s2	down	10G	9216	swp	
swp1s3	down	10G	9216	swp	
swp2s0	down	25G	9216	swp	
swp2s1	down	25G	9216	swp	
swp2s2	down	25G	9216	swp	
swp2s3	down	25G	9216	swp	
swp3	down		9216	swp	
swp4	down		9216	swp	
...					
...					
swp14	down		9216	swp	
swp15	up	100G	9216	swp	ossq-int-rcf10
swp15					
swp16	up	100G	9216	swp	ossq-int-rcf10
swp16					

1. Verifique 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

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	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					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

2. 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

3. Desconecte el cable del puerto del clúster e3b del nodo 1 y, a continuación, conecte e3b al puerto 3 del switch del clúster sw2, utilizando el cableado adecuado compatible con los switches SN2100.
4. Desconecte el cable del puerto del clúster e3b en el nodo 2 y, a continuación, conecte e3b al puerto 4 del switch del clúster sw2, utilizando el cableado adecuado compatible con los conmutadores SN2100.

Cumulus Linux 4.4.x

1. En el switch SW2, habilite todos los puertos orientados al nodo.

Los siguientes comandos habilitan los puertos orientados al nodo en el switch sw2:

```
cumulus@sw2:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link  
down  
cumulus@sw2:~$ net pending  
cumulus@sw2:~$ net commit
```

2. En el switch SW2, verifique que todos los puertos estén activos:

```
net show interface all
```

```
cumulus@sw2:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
...						
DN	swp1s0	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s1	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s2	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s3	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s0	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s1	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s2	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s3	25G	9216	Trunk/L2		Master:
br_default(UP)						
UP	swp3	100G	9216	Trunk/L2	node1 (e3b)	Master:
br_default(UP)						
UP	swp4	100G	9216	Trunk/L2	node2 (e3b)	Master:
br_default(UP)						
...						
...						
UP	swp15	100G	9216	BondMember	swp15	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	swp16	Master:
cluster_isl(UP)						
...						

3. En ambos conmutadores sw1 y SW2, verifique que ambos nodos tengan cada uno una conexión a cada conmutador:

```
net show lldp
```

En el siguiente ejemplo se muestran los resultados adecuados para ambos interruptores sw1 y sw2:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

Cumulus Linux 5.x

1. En el switch SW2, habilite todos los puertos orientados al nodo.

Los siguientes comandos habilitan los puertos orientados al nodo en el switch sw2:

```
cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
up  
cumulus@sw2:~$ nv config apply  
cumulus@sw2:~$ nv config save
```

2. En el switch SW2, verifique que todos los puertos estén activos:

```
nv show interface
```

```
cumulus@sw2:~$ nv show interface
```

Interface	State	Speed	MTU	Type	Remote Host
Remote Port	Summary				
-----	-----	-----	-----	-----	-----
...					
...					
swp1s0	up	10G	9216	swp	odq-a300-1a
e0a					
swp1s1	up	10G	9216	swp	odq-a300-1b
e0a					
swp1s2	down	10G	9216	swp	
swp1s3	down	10G	9216	swp	
swp2s0	down	25G	9216	swp	
swp2s1	down	25G	9216	swp	
swp2s2	down	25G	9216	swp	
swp2s3	down	25G	9216	swp	
swp3	down		9216	swp	
swp4	down		9216	swp	
...					
...					
swp14	down		9216	swp	
swp15	up	100G	9216	swp	ossq-int-rcf10
swp15					
swp16	up	100G	9216	swp	ossq-int-rcf10
swp16					

3. En ambos conmutadores sw1 y SW2, verifique que ambos nodos tengan cada uno una conexión a cada conmutador:

```
nv show interface --view=lldp
```

Los siguientes ejemplos muestran los resultados adecuados para los switches sw1 y SW2:

```
cumulus@sw1:~$ nv show interface --view=lldp
```

Interface	Speed	Type	Remote Host
Remote Port			
-----	-----	-----	-----
...			
...			
swp1s0	10G	swp	odq-a300-1a
e0a			

```

swp1s1      10G      swp      odq-a300-1b
e0a
swp1s2      10G      swp
swp1s3      10G      swp
swp2s0      25G      swp
swp2s1      25G      swp
swp2s2      25G      swp
swp2s3      25G      swp
swp3                swp
swp4                swp
...
...
swp14                swp
swp15      100G      swp      ossg-int-rcf10
swp15
swp16      100G      swp      ossg-int-rcf10
swp16

```

```
cumulus@sw2:~$ nv show interface --view=lldp
```

Interface	Speed	Type	Remote Host
Remote Port			
-----	-----	-----	-----

...			
...			
swp1s0	10G	swp	odq-a300-1a
e0a			
swp1s1	10G	swp	odq-a300-1b
e0a			
swp1s2	10G	swp	
swp1s3	10G	swp	
swp2s0	25G	swp	
swp2s1	25G	swp	
swp2s2	25G	swp	
swp2s3	25G	swp	
swp3		swp	
swp4		swp	
...			
...			
swp14		swp	
swp15	100G	swp	ossg-int-rcf10
swp15			
swp16	100G	swp	ossg-int-rcf10
swp16			

1. Muestra información sobre los dispositivos de red detectados en el cluster:

```
network device-discovery show -protocol lldp
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
-----
node1      /lldp
           e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3       -
           e3b    sw2 (b8:ce:f6:19:1b:96)   swp3       -
node2      /lldp
           e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4       -
           e3b    sw2 (b8:ce:f6:19:1b:96)   swp4       -
```

2. 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							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

Node: node2

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

Paso 3: Verificar la configuración

1. Activa la reversión automática en todos los LIF del clúster:

```
net interface modify -vserver Cluster -lif * -auto-revert true
```

Muestra el ejemplo

```
cluster1::*> net interface modify -vserver Cluster -lif * -auto
-revert true
```

Vserver	Logical Interface	Auto-revert
Cluster	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

2. Compruebe que se muestran todas las interfaces true para Is Home:

```
net interface show -vserver Cluster
```



Esto puede tardar un minuto 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::*> net interface show -vserver Cluster
```

Current Is	Logical Vserver	Status Interface	Network Admin/Oper Address/Mask	Current Node	Port	
Home						
	Cluster	node1_clus1	up/up	169.254.209.69/16	node1	e3a
true		node1_clus2	up/up	169.254.49.125/16	node1	e3b
true		node2_clus1	up/up	169.254.47.194/16	node2	e3a
true		node2_clus2	up/up	169.254.19.183/16	node2	e3b
true						

3. Compruebe que la configuración está desactivada:

```
network options switchless-cluster show
```

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
```

4. 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

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
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)

```

1. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

2. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

El futuro

["Configure la supervisión de estado del switch".](#)

Reemplace los interruptores

Sustituya un conmutador de clúster NVIDIA SN2100

Siga este procedimiento para sustituir un conmutador NVIDIA SN2100 defectuoso en una red de clúster. Este es un procedimiento no disruptivo (NDU).

Revise los requisitos

Infraestructura de red y clúster existente

Asegúrese de que:

- 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.
- La `ONTAP cluster ping-cluster -node node1` El comando indica que la conectividad básica y la comunicación más grande que PMTU se realizan correctamente en todas las rutas.

Conmutador de sustitución NVIDIA SN2100

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.
- Las conexiones de nodos son los puertos swp1 a swp14.
- Todos los puertos de enlace entre switches (ISL) están deshabilitados en los puertos swp15 y swp16.
- El archivo de configuración de referencia (RCF) y el interruptor de imagen del sistema operativo Cumulus se cargan en el conmutador.
- Se ha completado la personalización inicial del conmutador.

Asegúrese también de que cualquier personalización de sitio anterior, como STP, SNMP y SSH, se copie al nuevo switch.



Debe ejecutar el comando para migrar una LIF de clúster desde el nodo donde se aloja la LIF del clúster.

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después de las tareas de mantenimiento para deshabilitar la creación de casos durante el mantenimiento. Consulte este artículo de la base de conocimientos ["SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#) para obtener más detalles.
- Habilite el registro de sesiones para cualquier sesión de CLI. Para obtener instrucciones sobre cómo activar el registro de sesiones, consulte la sección «Salida de sesión de registro» de este artículo de la base de conocimientos ["Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP"](#).

Sustituya el interruptor

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los conmutadores NVIDIA SN2100 existentes son *sw1* y *sw2*.
- El nombre del nuevo switch NVIDIA SN2100 es *nsw2*.
- Los nombres de nodo son *1* y *2*.

- Los puertos de clúster de cada nodo se denominan *e3a* y *e3b*.
- Los nombres de LIF del clúster son *1_clus1* y *1_clus2* para los nodos 1, y *2_clus1* y *2_clus2* para los nodos 2.
- El prompt de cambios en todos los nodos del clúster es `cluster1::*>`
- Los puertos de arranque tienen el formato: `swp[Port]s[breakout Port 0-3]`. Por ejemplo, cuatro puertos de arranque en `swp1` son *swp1s0*, *swp1s1*, *swp1s2* y *swp1s3*.

Acerca de la topología de red del clúster

Este procedimiento se basa en la siguiente topología de red de clúster:

Mostrar topología de ejemplo

cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore						
						Speed(Mbps)
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						Status

e3a	Cluster	Cluster		up	9000	auto/100000
false						healthy
e3b	Cluster	Cluster		up	9000	auto/100000
false						healthy

Node: node2

Ignore						
						Speed(Mbps)
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						Status

e3a	Cluster	Cluster		up	9000	auto/100000
false						healthy
e3b	Cluster	Cluster		up	9000	auto/100000
false						healthy

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	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					


```

node2_clus1 up/up 169.254.47.194/16 node2 e3a
true
node2_clus2 up/up 169.254.19.183/16 node2 e3b
true

```

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/	Local	Discovered			
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform	
node1	/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-	
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-	
node2	/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-	
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-	

+

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	sw2	e3a
swp4	100G	Trunk/L2	sw2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	sw1	e3b
swp4	100G	Trunk/L2	sw1	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

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
```

donde x es la duración de la ventana de mantenimiento en horas.

2. Cambie el nivel de privilegio a avanzado, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

3. Instale el RCF y la imagen adecuados en el interruptor, nsw2, y realice las preparaciones necesarias del sitio.

Si es necesario, verifique, descargue e instale las versiones apropiadas del software RCF y Cumulus para el nuevo interruptor.

- a. Puede descargar el software Cumulus correspondiente para los switches de clúster del sitio *NVIDIA Support*. Siga los pasos de la página de descarga para descargar Cumulus Linux para la versión del software ONTAP que está instalando.
- b. El RCF adecuado está disponible en "[Cluster de NVIDIA y switches de almacenamiento](#)" página. Siga los pasos de la página de descarga para descargar el RCF correcto para la versión del software ONTAP que está instalando.

Paso 2: Configure los puertos y el cableado

Cumulus Linux 4.4.3

1. En el nuevo switch nsw2, inicie sesión como administrador y apague todos los puertos que se conectarán a las interfaces de clúster del nodo (puertos swp1 a swp14).

Los LIF de los nodos del clúster ya deberían haber realizado la conmutación al otro puerto del clúster para cada nodo.

```
cumulus@nsw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

2. Deshabilite la reversión automática en las LIF del clúster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

```
cluster1::~*> network interface modify -vserver Cluster -lif * -auto-revert false
```

Warning: Disabling the auto-revert feature of the cluster logical interface may effect the availability of your cluster network. Are you sure you want to continue? {y|n}: **y**

3. Verifique que todos los LIF del clúster tengan la reversión automática deshabilitada:

```
net interface show -vserver Cluster -fields auto-revert
```

4. Apague los puertos ISL swp15 y swp16 en el conmutador SN2100 sw1.

```
cumulus@sw1:~$ net add interface swp15-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

5. Retire todos los cables del conmutador SN2100 sw1 y, a continuación, conéctelos a los mismos puertos del conmutador SN2100 nsw2.
6. Suba los puertos ISL swp15 y swp16 entre los switches sw1 y nsw2.

Los siguientes comandos habilitan los puertos ISL swp15 y swp16 en el switch sw1:

```
cumulus@sw1:~$ net del interface swp15-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

En el siguiente ejemplo, se muestra que los puertos ISL están activos en la switch sw1:

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	----	-----	-----	-----	

...						
...						
UP	swp15	100G	9216	BondMember	nsw2 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	nsw2 (swp16)	Master: cluster_isl (UP)

En el siguiente ejemplo, se muestra que los puertos ISL están activos en el switch nsw2:

```
cumulus@nsw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	----	-----	-----	-----	

...						
...						
UP	swp15	100G	9216	BondMember	sw1 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	sw1 (swp16)	Master: cluster_isl (UP)

7. Compruebe que el puerto e3b está activo en todos los nodos:

```
network port show -ip space Cluster
```

La salida debe ser similar a la siguiente:

```
cluster1::*> network port show -ipspace Cluster
```

Node: node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

8. Los puertos de clúster de cada nodo ahora están conectados a los switches de clúster del siguiente modo, desde la perspectiva de los nodos:

```
cluster1::~*> network device-discovery show -protocol lldp
```

Node/	Local	Discovered			
Protocol	Port	Device	(LLDP: ChassisID)	Interface	Platform

node1	/lldp				
	e3a	sw1	(b8:ce:f6:19:1a:7e)	swp3	-
	e3b	nsw2	(b8:ce:f6:19:1b:b6)	swp3	-
node2	/lldp				
	e3a	sw1	(b8:ce:f6:19:1a:7e)	swp4	-
	e3b	nsw2	(b8:ce:f6:19:1b:b6)	swp4	-

9. Compruebe que todos los puertos de clúster del nodo estén activos:

```
net show interface
```

```
cumulus@nsw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

10. Compruebe que ambos nodos tengan una conexión cada uno con cada switch:

```
net show lldp
```

En el siguiente ejemplo, se muestran los resultados adecuados para ambos switches:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

```
cumulus@nsw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

11. Habilite la reversión automática en las LIF del clúster:

```
cluster1::~*> network interface modify -vserver Cluster -lif * -auto-revert true
```

12. En el switch nsw2, conecte los puertos conectados a los puertos de red de los nodos.

```
cumulus@nsw2:~$ net del interface swp1-14 link down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

13. Muestra información sobre los nodos de un clúster:

```
cluster show
```

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	true	true
node2	true	true

14. Compruebe que todos los puertos físicos del clúster estén en funcionamiento:

```
network port show ipspace Cluster
```

```
cluster1::*> network port show -ipspace Cluster
```

Node node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Cumulus Linux 5.x

1. En el nuevo switch nsw2, inicie sesión como administrador y apague todos los puertos que se conectarán a las interfaces de clúster del nodo (puertos swp1 a swp14).

Los LIF de los nodos del clúster ya deberían haber realizado la conmutación al otro puerto del clúster para cada nodo.

```
cumulus@nsw2:~$ nv set interface swp15-16 link state down
cumulus@nsw2:~$ nv config apply
```

2. Deshabilite la reversión automática en las LIF del clúster:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```



```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

Warning: Disabling the auto-revert feature of the cluster logical interface may effect the availability of your cluster network. Are you sure you want to continue? {y|n}: **y**

3. Verifique que todos los LIF del clúster tengan la reversión automática deshabilitada:

```
network interface show -vserver Cluster -fields auto-revert
```

4. Apague los puertos ISL swp15 y swp16 en el conmutador SN2100 sw1.

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

5. Retire todos los cables del conmutador SN2100 sw1 y, a continuación, conéctelos a los mismos puertos del conmutador SN2100 nsw2.
6. Suba los puertos ISL swp15 y swp16 entre los switches sw1 y nsw2.

Los siguientes comandos habilitan los puertos ISL swp15 y swp16 en el switch sw1:

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

En el siguiente ejemplo, se muestra que los puertos ISL están activos en la switch sw1:

```
cumulus@sw1:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
----	-----	----	-----	-----	-----	
...						
...						
UP	swp15	100G	9216	BondMember	nsw2 (swp15)	Master: cluster_isl (UP)
UP	swp16	100G	9216	BondMember	nsw2 (swp16)	Master: cluster_isl (UP)

En el siguiente ejemplo, se muestra que los puertos ISL están activos en el switch nsw2:

```
cumulus@nsw2:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	

...						
...						
UP	swp15	100G	9216	BondMember	sw1 (swp15)	Master:
	cluster_isl (UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)	Master:
	cluster_isl (UP)					

7. Compruebe que el puerto e3b está activo en todos los nodos:

```
network port show -ipspace Cluster
```

La salida debe ser similar a la siguiente:

```
cluster1::*> network port show -ipspace Cluster
```

Node: node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

8. Los puertos de clúster de cada nodo ahora están conectados a los switches de clúster del siguiente modo, desde la perspectiva de los nodos:

```
cluster1::~*> network device-discovery show -protocol lldp
```

Node/	Local	Discovered			
Protocol	Port	Device	(LLDP: ChassisID)	Interface	Platform

node1	/lldp				
	e3a	sw1	(b8:ce:f6:19:1a:7e)	swp3	-
	e3b	nsw2	(b8:ce:f6:19:1b:b6)	swp3	-
node2	/lldp				
	e3a	sw1	(b8:ce:f6:19:1a:7e)	swp4	-
	e3b	nsw2	(b8:ce:f6:19:1b:b6)	swp4	-

9. Compruebe que todos los puertos de clúster del nodo estén activos:

```
nv show interface
```

```
cumulus@nsw2::~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp3	100G	9216	Trunk/L2	
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	
Master: bridge(UP)					
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master: cluster_isl(UP)					
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master: cluster_isl(UP)					

10. Compruebe que ambos nodos tengan una conexión cada uno con cada switch:

```
nv show interface lldp
```

En el siguiente ejemplo, se muestran los resultados adecuados para ambos switches:

```
cumulus@sw1:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

```
cumulus@nsw2:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

11. Habilite la reversión automática en las LIF del clúster:

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert  
true
```

12. En el switch nsw2, conecte los puertos conectados a los puertos de red de los nodos.

```
cumulus@nsw2:~$ nv set interface swp1-14 link state up  
cumulus@nsw2:~$ nv config apply
```

13. Muestra información sobre los nodos de un clúster:

```
cluster show
```

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	true	true
node2	true	true

14. Compruebe que todos los puertos físicos del clúster estén en funcionamiento:

```
network port show ipspace Cluster
```

```
cluster1::*> network port show -ipspace Cluster
```

Node node1

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Node: node2

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/10000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/10000
healthy	false					

Paso 3: Verificar la configuración

Cumulus Linux 4.4.3

1. Compruebe que la red de clúster esté en buen estado.

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

Cumulus Linux 5.x

1. Compruebe que la red de clúster esté en buen estado.

```
cumulus@sw1:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

1. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

2. 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
```

El futuro

["Configure la supervisión de estado del switch".](#)

Sustituya los switches de clúster NVIDIA SN2100 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.

Antes de empezar

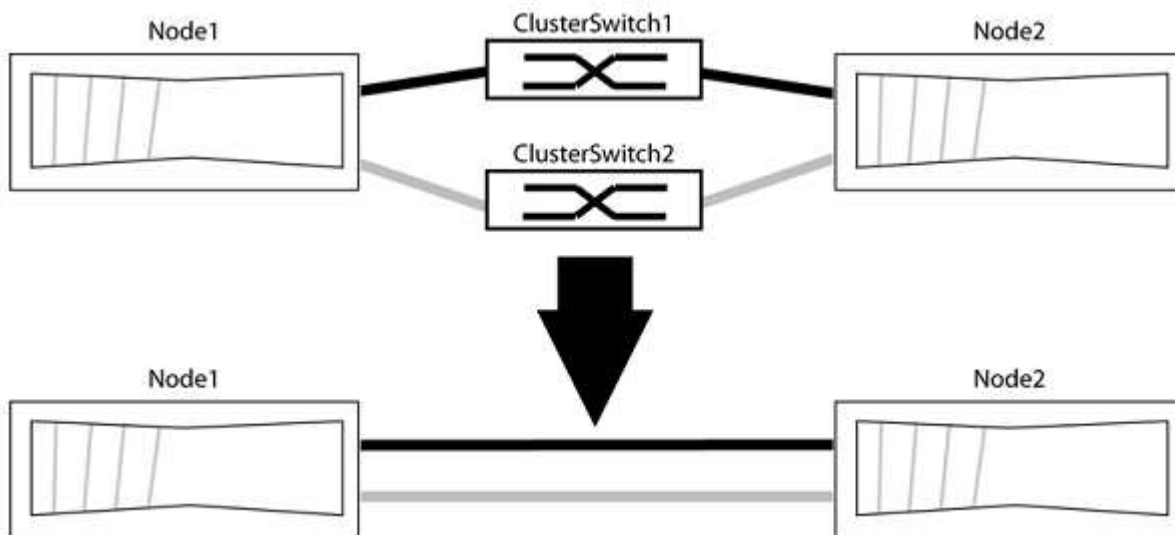
Asegúrese de tener lo siguiente:

- 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

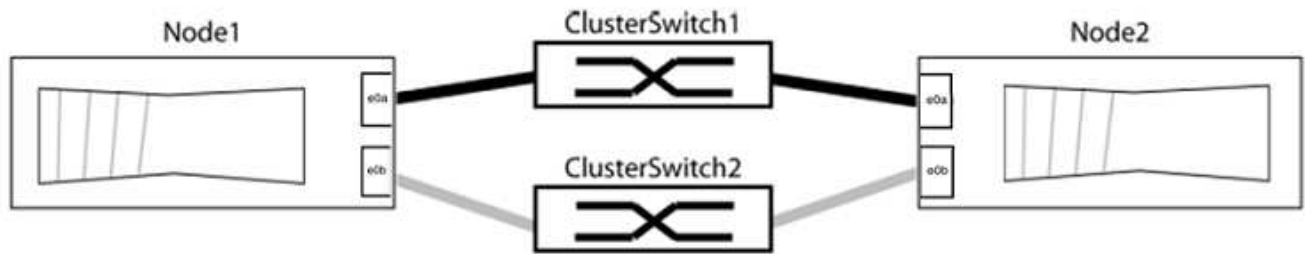
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

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 de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					

node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Verifique que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

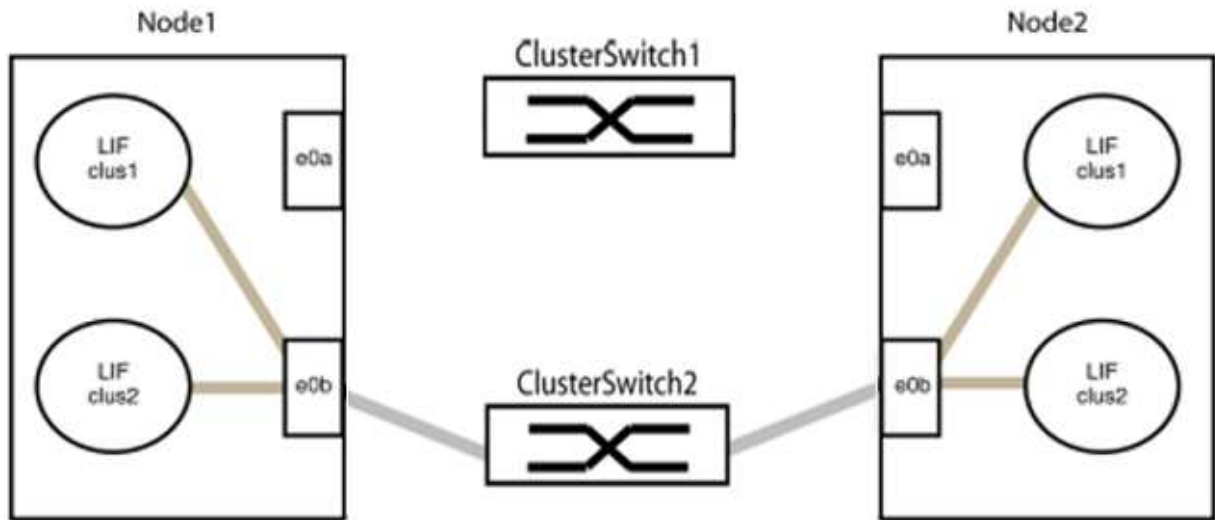
2. Configure la configuración sin switches para los puertos del grupo 1.



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**.

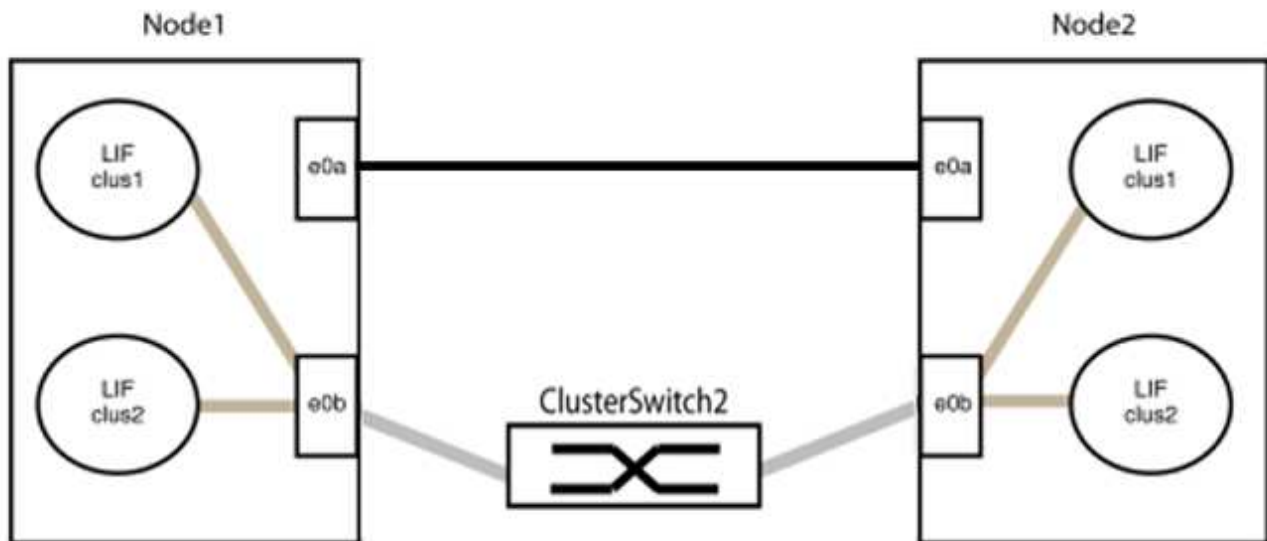
- a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

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:



3. 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
```

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```



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.

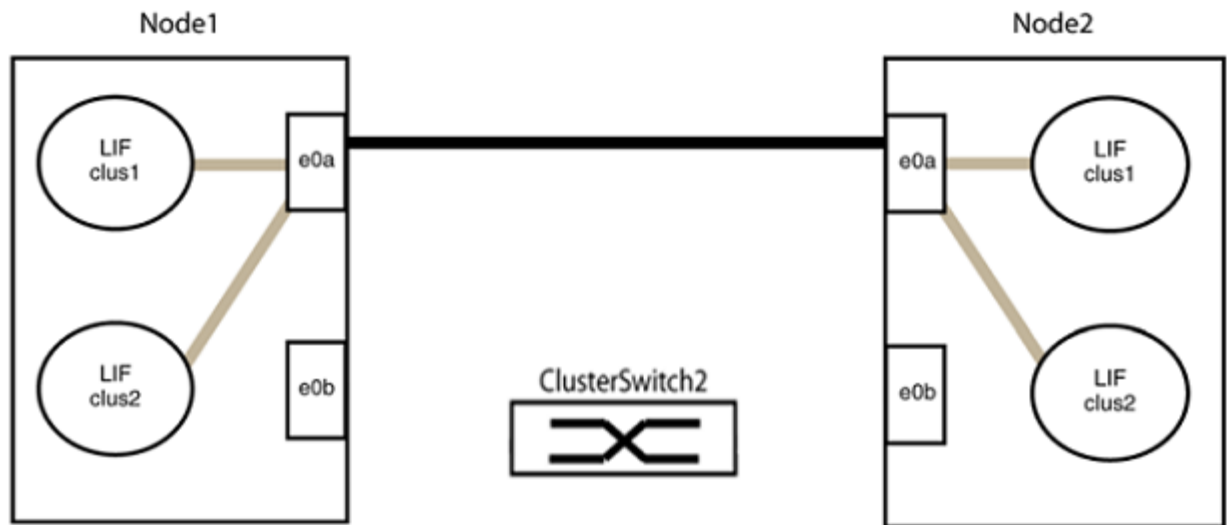
1. Configure la configuración sin switch para los puertos del grupo 2.



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**.

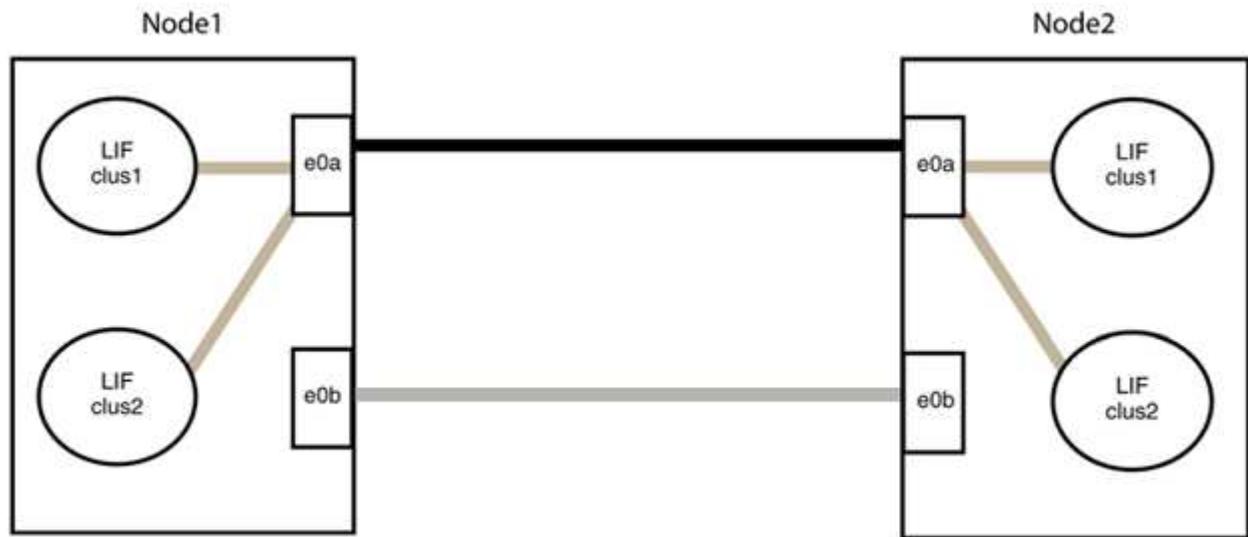
- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

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 épsilon en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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"](#).

2. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

Switches de almacenamiento

Cisco Nexus 9336C-FX2 o 9336C-FX2-T

Manos a la obra

Flujo de trabajo de instalación y configuración para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 9336C-FX2-T

Los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T son parte de la plataforma Cisco Nexus 9000 y se pueden instalar en un gabinete de sistema NetApp .

Cisco Nexus 9336C-FX2 (36 puertos) es un conmutador de datos/almacenamiento/clúster de alta densidad de puertos. Cisco Nexus 9336C-FX2-T (12 puertos) es un conmutador de alto rendimiento y baja densidad de puertos que admite configuraciones 10/25/40/100 GbE.

Siga estos pasos de flujo de trabajo para instalar y configurar sus conmutadores Cisco 9336C-FX2 y 9336C-FX2-T.

1

"Revisar los requisitos de configuración"

Revise los requisitos de configuración para los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

2

"Revise los componentes y números de pieza"

Revise los componentes y números de pieza de los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

3

"Revisar la documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar los conmutadores 9336C-FX2 y 9336C-FX2-T y el clúster ONTAP .

4

"Revisar los requisitos de Smart Call Home"

Revise los requisitos de la función Cisco Smart Call Home, que se utiliza para monitorear los componentes de hardware y software de su red.

5

"Instale el hardware"

Instale el hardware del interruptor.

6

"Configurar el software"

Configurar el software del conmutador.

Requisitos de configuración para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para la instalación y el mantenimiento de los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T, asegúrese de revisar la configuración y los requisitos de red.

Soporte de ONTAP

ONTAP 9.9.1 y versiones posteriores

Desde ONTAP 9.9.1, puede utilizar los switches Cisco Nexus 9336C-FX2 para combinar la funcionalidad de almacenamiento y clúster en una configuración de switch compartido.

Si desea crear clústeres de ONTAP con más de dos nodos, necesita dos switches de red compatibles.



El monitor de estado del switch Ethernet no admite ONTAP 9.13.1P8 y versiones anteriores y 9.14.1P3 y anteriores o NX-OS versión 10,3(4a)(M).

ONTAP 9.10.1 y posteriores

Además, a partir de ONTAP 9.10.1, puede utilizar los conmutadores Cisco Nexus 9336C-FX2-T para combinar la funcionalidad de almacenamiento y clúster en una configuración de conmutador compartido.

Si desea crear clústeres de ONTAP con más de dos nodos, necesita dos switches de red compatibles.

Requisitos de configuración

Para la configuración, necesita el número y tipo adecuados de cables y conectores de cable para los conmutadores.

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 AFF A700 de AFF, la interfaz e0M utiliza un puerto Ethernet dedicado.
- Consulte la ["Hardware Universe"](#) para obtener la información más reciente.

Para obtener más información acerca de la configuración inicial del switch, consulte la siguiente guía: ["Guía de instalación y actualización de Cisco Nexus 9336C-FX2"](#).

¿Qué sigue?

Después de revisar los requisitos de configuración, puede confirmar su ["componentes y números de pieza"](#).

Componentes y números de pieza para Cisco switches de almacenamiento Nexus 9336C-FX2 y 9336C-FX2-T.

Para la instalación y el mantenimiento de switches de almacenamiento Nexus 9336C-FX2 y 9336C-FX2-T de Cisco, asegúrese de revisar la lista de componentes y números de pieza.

En la siguiente tabla, se enumeran el número de pieza y la descripción de los switches de almacenamiento 9336C-FX2 y 9336C-FX2-T, los ventiladores y las fuentes de alimentación:

Número de pieza	Descripción
X190200-CS-PE	Switch de cluster, N9336C 36Pt PTSX 10/25/40/100g
X190200-CS-PI	Conmutador de grupo, N9336C 36Pt PSIN 10/25/40/100g
X190212-CS-PE	Switch de cluster, N9336C 12pt (9336C-FX2-T) PTSX 10/25/40/100g
X190212-CS-PI	Conmutador de grupo de instrumentos, N9336C 12pt (9336C-FX2-T) PSIN 10/25/40/100g
SW-N9K-FX2-24P-UPG	SW, Cisco 9336CFX2, licencia POD de 24 puertos
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40 GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100 GQSFP28
X190002	Kit de accesorios X190001/X190003
X-NXA-PAC-1100W-PE2	Fuente de alimentación de 1100 W ac N9K-9336C: Flujo de aire de escape lateral del puerto
X-NXA-PAC-1100W-PI2	Fuente de alimentación de 1100 W ac N9K-9336C - flujo de aire de entrada lateral del puerto
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, flujo de aire del lado de la lumbrera
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, flujo de aire de entrada lateral de la lumbrera

Licencias inteligentes de Cisco solo para puertos 9336C-FX2-T

Para activar más de 12 puertos en su switch de almacenamiento Cisco Nexus 9336C-FX-T, debe comprar una licencia inteligente de Cisco. Las licencias inteligentes de Cisco se administran a través de cuentas inteligentes de Cisco.

1. Cree una nueva cuenta Smart, si es necesario. Consulte ["Cree una nueva cuenta Smart"](#) para obtener más información.
2. Solicitar acceso a una cuenta Smart existente. Consulte ["Solicitar acceso a una cuenta Smart existente"](#) para obtener más información.



Una vez que haya adquirido su licencia Smart, instale el RCF adecuado para habilitar y configurar todos los 36 puertos disponibles para su uso.

¿Qué sigue?

Después de haber confirmado sus componentes y números de pieza, revise el ["documentación requerida"](#) .

Requisitos de documentación para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para la instalación y el mantenimiento de los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T, asegúrese de revisar la documentación específica del conmutador y del controlador para configurar los conmutadores Cisco 9336-FX2 y el clúster ONTAP .

Documentación de los switches

Para configurar los switches Cisco Nexus 9336C-FX2, necesita la siguiente documentación del ["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.

Título del documento	Descripción
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 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 9336-FX2 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 un switch Cisco 9336-FX2 en un armario de NetApp"	Describe cómo instalar un switch Cisco Nexus 9336C-FX2 en un armario de cuatro parantes de NetApp.

Requisitos de Smart Call Home

Para utilizar Smart Call Home, debe configurar un conmutador de red de clúster para comunicarse mediante correo electrónico con el sistema Smart Call Home. Además, puede configurar opcionalmente su conmutador de red de clúster para aprovechar la función de soporte Smart Call Home integrada de Cisco.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Antes de poder utilizar Smart Call Home, tenga en cuenta los siguientes requisitos:

- Debe haber un servidor de correo electrónico.
- 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

Flujo de trabajo de instalación de hardware para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para instalar y configurar el hardware de los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T, siga estos pasos:

1

"Complete la hoja de trabajo de cableado"

La hoja de cálculo de cableado de 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 el interruptor"

Instale los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

3

"Instale el interruptor en un armario NetApp"

Instale los conmutadores 9336C-FX2 y 9336C-FX2-T y el panel de paso en un gabinete NetApp según sea necesario.

Complete la hoja de datos de cableado de Nexus 9336C-FX2 o 9336C-FX2-T de Cisco

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 muestras 9336C-FX2](#)
- [Hoja de trabajo para el cableado en blanco 9336C-FX2](#)
- [Hoja de datos para el cableado de muestras 9336C-FX2-T \(12 puertos\)](#)

- [Hoja de datos para el cableado en blanco de 9336C-FX2-T \(12 puertos\)](#)

Hoja de trabajo para el cableado de muestras 9336C-FX2

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 de 100 GbE 1	1	4 nodos de 100 GbE 1
2	4 nodos de 100 GbE 2	2	4 nodos de 100 GbE 2
3	4 nodos de 100 GbE 3	3	4 nodos de 100 GbE 3
4	4 nodos de 100 GbE 4	4	4 nodos de 100 GbE 4
5	4 nodos de 100 GbE 5	5	4 nodos de 100 GbE 5
6	4 nodos de 100 GbE 6	6	4 nodos de 100 GbE 6
7	4 nodos de 100 GbE 7	7	4 nodos de 100 GbE 7
8	4 nodos de 100 GbE 8	8	4 nodos de 100 GbE 8
9	4 nodos de 100 GbE 9	9	4 nodos de 100 GbE 9
10	4 nodos de 100 GbE 10	10	4 nodos de 100 GbE 10
11	4 nodos de 100 GbE 11	11	4 nodos de 100 GbE 11
12	4 nodos de 100 GbE 12	12	4 nodos de 100 GbE 12
13	4 nodos de 100 GbE 13	13	4 nodos de 100 GbE 13
14	4 nodos de 100 GbE 14	14	4 nodos de 100 GbE 14
15	4 nodos de 100 GbE 15	15	4 nodos de 100 GbE 15
16	4 nodos de 100 GbE 16	16	4 nodos de 100 GbE 16
17	4 nodos de 100 GbE 17	17	4 nodos de 100 GbE 17
18	4 nodos de 100 GbE 18	18	4 nodos de 100 GbE 18

Switch de clúster a		Switch del clúster B	
19	4 nodos de 100 GbE 19	19	4 nodos de 100 GbE 19
20	4 nodos de 100 GbE 20	20	4 nodos de 100 GbE 20
21	4 nodos de 100 GbE 21	21	4 nodos de 100 GbE 21
22	4 nodos de 100 GbE 22	22	4 nodos de 100 GbE 22
23	4 nodos de 100 GbE 23	23	4 nodos de 100 GbE 23
24	4 nodos de 100 GbE 24	24	4 nodos de 100 GbE 24
25	4 nodos de 100 GbE 25	25	4 nodos de 100 GbE 25
26	4 nodos de 100 GbE 26	26	4 nodos de 100 GbE 26
27	4 nodos de 100 GbE 27	27	4 nodos de 100 GbE 27
28	4 nodos de 100 GbE 28	28	4 nodos de 100 GbE 28
29	4 nodos de 100 GbE 29	29	4 nodos de 100 GbE 29
30	4 nodos de 100 GbE 30	30	4 nodos de 100 GbE 30
31	4 nodos de 100 GbE 31	31	4 nodos de 100 GbE 31
32	4 nodos de 100 GbE 32	32	4 nodos de 100 GbE 32
33	4 nodos de 100 GbE 33	33	4 nodos de 100 GbE 33
30	4 nodos de 100 GbE 30	30	4 nodos de 100 GbE 33
34	4 nodos de 100 GbE 34	34	4 nodos de 100 GbE 34
35	4 nodos de 100 GbE 35	35	4 nodos de 100 GbE 35
36	4 nodos de 100 GbE 36	36	4 nodos de 100 GbE 36

Hoja de trabajo para el cableado en blanco 9336C-FX2

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	
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	
20		20	
21		21	
22		22	

Switch de clúster a		Switch del clúster B	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	

Hoja de datos para el cableado de muestras 9336C-FX2-T (12 puertos)

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 de 100 GbE 1	1	4 nodos de 100 GbE 1
2	4 nodos de 100 GbE 2	2	4 nodos de 100 GbE 2
3	4 nodos de 100 GbE 3	3	4 nodos de 100 GbE 3
4	4 nodos de 100 GbE 4	4	4 nodos de 100 GbE 4

Switch de clúster a		Switch del clúster B	
5	4 nodos de 100 GbE 5	5	4 nodos de 100 GbE 5
6	4 nodos de 100 GbE 6	6	4 nodos de 100 GbE 6
7	4 nodos de 100 GbE 7	7	4 nodos de 100 GbE 7
8	4 nodos de 100 GbE 8	8	4 nodos de 100 GbE 8
9	4 nodos de 100 GbE 9	9	4 nodos de 100 GbE 9
10	4 nodos de 100 GbE 10	10	4 nodos de 100 GbE 10
11 a 36	Requiere licencia	11 hasta 36	Requiere licencia

Hoja de datos para el cableado en blanco de 9336C-FX2-T (12 puertos)

Puede utilizar la hoja de datos de cableado vacía para documentar las plataformas que se admiten como nodos de un clúster.

Switch de clúster a		Switch del clúster B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11 hasta 36	Requiere licencia	11 hasta 36	Requiere licencia

Consulte "[Hardware Universe](#)" para obtener más información sobre los puertos de switch.

¿Qué sigue?

Después de haber completado las hojas de trabajo de cableado, ["instalar el interruptor"](#) .

Instalar los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T

Siga este procedimiento para instalar los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T.

Antes de empezar

Asegúrese de tener lo siguiente:

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones 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.
- Las licencias aplicables, la información de configuración y red, y los cables.
- Completado ["hojas de datos para el cableado"](#).
- Los RCF de red de gestión y red de clúster de NetApp aplicables descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#). 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.
- Documentación del switch requerida. Consulte ["Documentación requerida"](#) si quiere más información.

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 9336C-FX2 en un armario de sistemas de NetApp	Consulte "Instale el switch en el armario de NetApp" 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.

El futuro

Opcionalmente, puedes ["Instale un switch Cisco Nexus 9336C-FX2 en un armario de NetApp"](#) . De lo contrario, vaya a ["configurar el conmutador"](#) .

Instalar los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T en un gabinete NetApp

Dependiendo de su configuración, es posible que necesite instalar los conmutadores Cisco Nexus 9336C-FX2 9336C-FX2-T y el panel de paso en un gabinete NetApp . Los soportes estándar se incluyen con el interruptor.

Antes de empezar

Asegúrese de tener lo siguiente:

- Para cada interruptor, debe suministrar los ocho tornillos 10-32 ó 12-24 y tuercas de abrazadera para montar los soportes y rieles deslizantes en los postes del armario delantero y trasero.
- Debe utilizar el kit de raíl estándar de Cisco para instalar el switch en un armario 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).

Documentación requerida

Revise los requisitos iniciales de preparación, el contenido del kit y las precauciones de seguridad en la ["Guía de instalación de hardware de Cisco Nexus serie 9000"](#).

Pasos

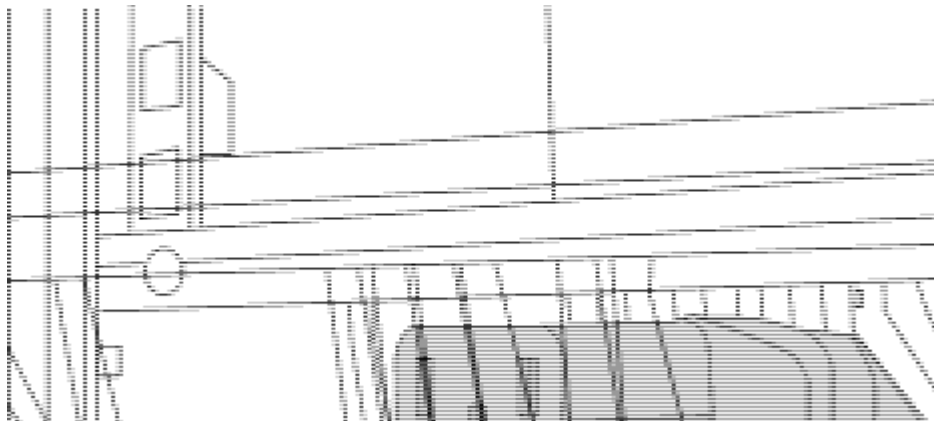
1. Instale el panel de borrado de paso en el armario de NetApp.

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.

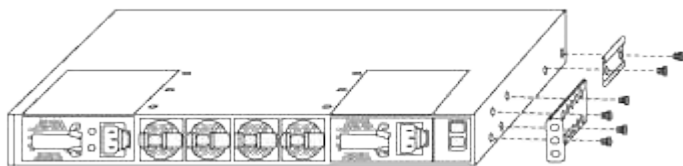
En este procedimiento, el panel de limpieza se instalará en U40.
 - ii. Instale dos tuercas de abrazadera a cada lado en los orificios cuadrados adecuados para los rieles delanteros del armario.
 - iii. Centre el panel verticalmente para evitar intrusiones en el espacio adyacente del bastidor y, a continuación, 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.



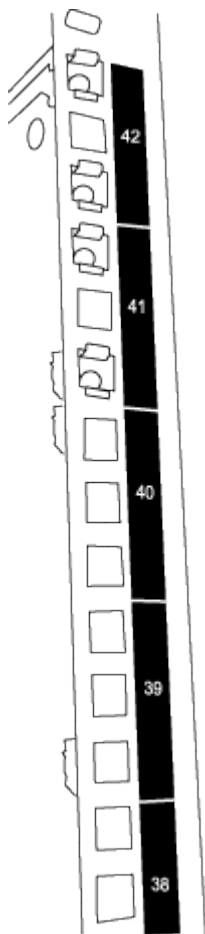
(1) conector hembra del cable puente.

2. Instale los soportes de montaje en rack en el chasis del switch Nexus 9336C-FX2.

- 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.



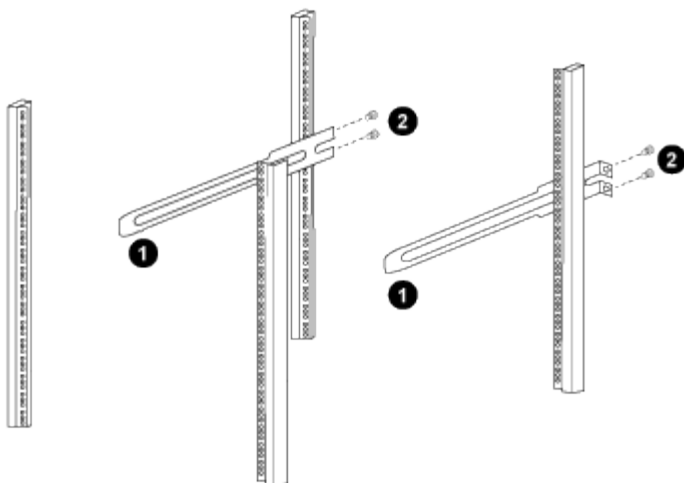
- b. Repita el paso 2a con el otro soporte de montaje en bastidor delantero en el otro lado del interruptor.
- c. Instale el soporte de montaje en bastidor trasero en el chasis del interruptor.
- d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del interruptor.
3. Instale las tuercas de abrazadera en las ubicaciones de los orificios cuadrados de los cuatro postes de IEA.



Los dos conmutadores 9336C-FX2 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.

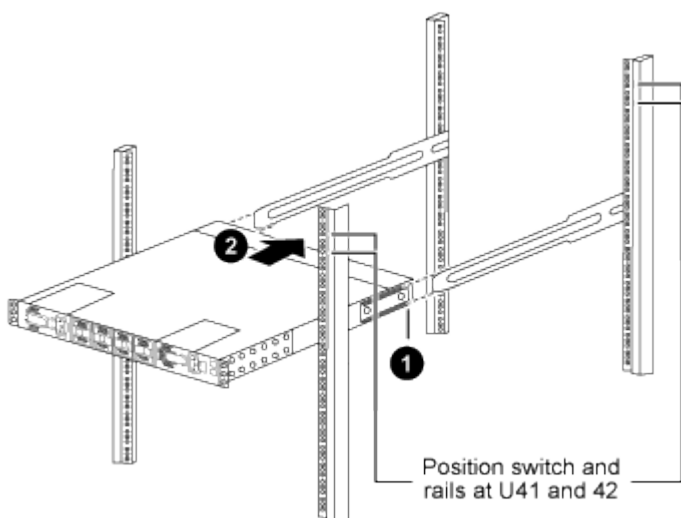
b. Repita los pasos 4a y 4b en las ubicaciones RU41 del armario.

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.

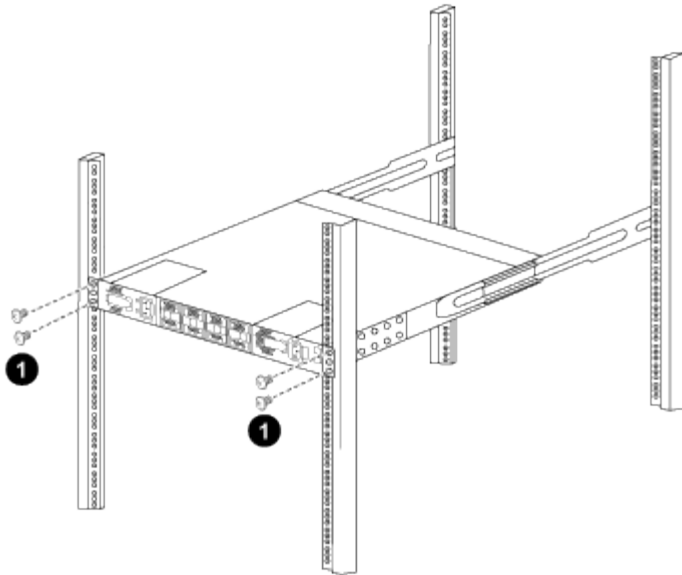
a. Coloque la parte posterior del interruptor en RU41.



(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 delantera 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 9336C-FX2 a cualquiera de los switches de administración (si se 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.

¿Qué sigue?

Después de haber instalado los conmutadores en el gabinete NetApp, "[configurar los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T](#)".

Configurar el software

Flujo de trabajo de instalación de software para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Para instalar y configurar el software para los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T, siga estos pasos:

1**"Configure el switch"**

Configure los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

2**"Prepárese para instalar el software NX-OS y RCF"**

El software Cisco NX-OS y los archivos de configuración de referencia (RCF) deben instalarse en los conmutadores de almacenamiento Cisco 9336C-FX2 y 9336C-FX2-T.

3**"Instale o actualice el software NX-OS"**

Descargue e instale o actualice el software NX-OS en los conmutadores de almacenamiento Cisco 9336C-FX2 y 9336C-FX2-T.

4**"Instale o actualice el RCF"**

Instale o actualice el RCF después de configurar los conmutadores Cisco 9336C-FX2 y 9336C-FX2-T por primera vez. También puede utilizar este procedimiento para actualizar su versión de RCF.

5**"Compruebe la configuración de SSH"**

Verifique que SSH esté habilitado en los conmutadores para usar el Monitor de estado del conmutador Ethernet (CSHM) y las funciones de recopilación de registros.

6**"Restablecer el interruptor a los valores predeterminados de fábrica"**

Borre las configuraciones de los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T.

Configurar los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T

Siga este procedimiento para configurar los conmutadores Cisco Nexus 9336C-FX2 y 9336C-FX2-T.

Antes de empezar

Asegúrese de tener lo siguiente:

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones 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.
- Las licencias aplicables, la información de configuración y red, y los cables.
- Completado ["hojas de datos para el cableado"](#).
- Los RCF de red de gestión y red de clúster de NetApp aplicables descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#). 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.
- Documentación del switch requerida. Consulte ["Documentación requerida"](#) si quiere más información.

Pasos

1. 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)	Responda con sí. El valor predeterminado es yes.  Se recomienda SSH cuando se utiliza Ethernet Switch Health Monitor (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.
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 a 2048.
¿Configurar el servidor NTP? (sí/no)	Responda con no . El valor predeterminado es no
Configuración de 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)	Responda con sí para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.  Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador.

- Compruebe las opciones de configuración que ha realizado en la pantalla que aparece al final de la instalación y asegúrese de guardar la configuración.

3. 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

Después de haber configurado sus conmutadores, ["Prepárese para instalar el software NX-OS y RCF"](#) .

Prepárese para instalar o actualizar el software NX-OS y RCF

Antes de instalar el software NX-OS y el archivo de configuración de referencia (RCF), siga este procedimiento.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de nodo son cluster1-01 y cluster1-02.
- Los nombres de las LIF de 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 9000; 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 lldp
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/lldp				
	e0a	cs1	Eth1/2	N9K-
C9336C				
	e0b	cs2	Eth1/2	N9K-
C9336C				
cluster1-01/lldp				
	e0a	cs1	Eth1/1	N9K-
C9336C				
	e0b	cs2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

4. Compruebe el estado administrativo u operativo de cada interfaz 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
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-01
```

```
Ignore
```

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	----	----	-----
e0a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
4 entries were displayed.
```

b. Mostrar información 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. Compruebe la conectividad de las interfaces del clúster remoto:

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
cluster1::*> network interface check cluster-connectivity start
```

```

cluster1::*> network interface check cluster-connectivity show

```

				Source	Destination
Packet					
Node	Date			LIF	LIF
Loss					
-----	-----	-----	-----	-----	-----
-----	-----	-----	-----		
node1	3/5/2024	19:21:18	-06:00	cluster1-01_clus2	cluster1-02
clus1	none				
	3/5/2024	19:21:20	-06:00	cluster1-01_clus2	cluster1-
02_clus2	none				
node2					
	3/5/2024	19:21:18	-06:00	cluster1-02_clus2	cluster1-
01_clus1	none				
	3/5/2024	19:21:20	-06:00	cluster1-02_clus2	cluster1-
01 clus2	none				

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

899

```

cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. Verifique que el comando de reversión automática esté habilitado en todas las LIF 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.

El futuro

Una vez que se haya preparado para instalar el software NX-OS y RCF, debe ["instalar o actualizar el software NX-OS"](#).

Instale o actualice el software NX-OS

Siga este procedimiento para instalar el software NX-OS en los conmutadores Nexus 9336C-FX2 y 9336C-FX2-T.

Antes de comenzar, complete el procedimiento en ["Prepare la instalación de NX-OS y RCF"](#).

Revise los requisitos

Antes de empezar

Asegúrese de tener lo siguiente:

- 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

- ["Página del switch Cisco Ethernet"](#)

Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.

- ["Guías de actualización y degradación de software"](#)

Consulte las guías de software y actualización correspondientes disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación del conmutador Cisco.

- ["Matriz de ISSU y actualización de Cisco Nexus 9000 y 3000"](#)

Proporciona información sobre actualización/degradación disruptiva para software Cisco NX-OS en los

switches de la serie Nexus 9000
en función de tus versiones actuales y objetivo.

En la página, selecciona **Actualización disruptiva** y selecciona tu versión actual y la versión de destino de la lista desplegable.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de nodo son cluster1-01, cluster1-02, cluster1-03 y cluster1-04.
- Los nombres de las 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.

Instale el software

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.

Pasos

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el comando ping 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 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. 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      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C-FX2
cluster1::*>
```

4. Compruebe el estado administrativo y operativo de cada puerto del clúster.

a. Compruebe que todos los puertos del clúster están **up** con un 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                                     Type                                     Address
Model
-----
cs1                                     cluster-network                         10.233.205.90      N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                     cluster-network                         10.233.205.91      N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

6. Copie las imágenes del software NX-OS y EPLD en el switch Nexus 9336C-FX2.

Muestra el ejemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. 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 08.38
  NXOS: version 9.3(4)
  BIOS compile time: 05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]

Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash: 53298520 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

8. Instale la imagen NX-OS.

La instalación del archivo de imagen hace que se cargue cada vez que se reinicia el conmutador.

Muestra el ejemplo

```
cs2# install all nxos bootflash:nxos.9.3.5.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

```
Verifying image type.  
[] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.  
[] 100% -- SUCCESS
```

```
Performing module support checks.  
[] 100% -- SUCCESS
```

```
Notifying services about system upgrade.  
[] 100% -- SUCCESS
```

Compatibility check is done:

Module	Bootable	Impact	Install-type	Reason
1	yes	Disruptive	Reset	Default upgrade is not hitless

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-
Version		Upg-Required	
1	nxos	9.3(4)	9.3(5)
yes			
1	bios	v08.37(01/28/2020):v08.23(09/23/2015)	
v08.38(05/29/2020)		yes	

```
Switch will be reloaded for disruptive upgrade.
```

```
Do you want to continue with the installation (y/n)? [n] y
```

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[ ] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[ ] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[ ] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[ ] 100% -- SUCCESS
```

```
Finishing the upgrade, switch will reboot in 10 seconds.
```

9. 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 05.33
NXOS: version 9.3(5)
BIOS compile time: 09/08/2018
NXOS image file is: bootflash:///nxos.9.3.5.bin
NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

```
cisco Nexus9000 C9336C-FX2 Chassis
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
Processor Board ID FOC20291J6K

Device name: cs2
bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
```

```
Reason: Reset due to upgrade
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

10. Actualice la imagen 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.9.3.5.img module all
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

11. Tras reiniciar el 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

12. 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 -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
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

cluster1-01/cdp	e0a	cs1	Ethernet1/7	N9K-
C9336C-FX2	e0d	cs2	Ethernet1/7	N9K-
C9336C-FX2				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C-FX2	e0d	cs2	Ethernet1/8	N9K-
C9336C-FX2				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/1	N9K-
C9336C-FX2				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/2	N9K-
C9336C-FX2				

```
cluster1::*> system cluster-switch show -is-monitoring-enabled  
-operational true
```

Switch Model	Type	Address	

cs1 C9336C-FX2	cluster-network	10.233.205.90	N9K-
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	N9K-

```

C9336C-FX2
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

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.

```

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 6 a 13 para instalar el software NX-OS en el interruptor CS1.

15. Habilite la reversión automática en las LIF del clúster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

16. 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 LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

El futuro

Después de haber instalado o actualizado el software NX-OS, ["instalar o actualizar el RCF"](#) .

Instale o actualice el archivo de configuración de referencia

Debe instalar el archivo de configuración de referencia (RCF) después de configurar los conmutadores de almacenamiento Nexus 9336C-FX2 y 9336C-FX2-T por primera vez.

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión"](#)

de [Cisco manteniendo la conectividad remota](#)" para obtener más información al instalar el RCF.

Antes de empezar

Compruebe las siguientes instalaciones y conexiones:

- Una conexión de consola al interruptor. La conexión de la consola es opcional si tiene acceso remoto al conmutador.
- El switch CS1 y el switch CS2 se encienden y la configuración inicial del switch se ha completado (la dirección IP de gestión y SSH está configurada).
- Se ha instalado la versión deseada de NX-OS.
- Los puertos del clúster de nodos de ONTAP no están conectados.

Paso 1: Instale el RCF en los interruptores

1. Inicie sesión en el switch CS1 mediante SSH o mediante una consola de serie.
2. Copie el RCF al bootflash del switch CS1 usando 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 9000"](#).

Muestra el ejemplo

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Storage.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

3. Aplique el RCF descargado 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 9000"](#).

Muestra el ejemplo

Este ejemplo muestra el RCF Nexus_9336C_RCF_v1.6-Storage.txt que se está instalando en el switch CS1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-
commands
```

4. Examine el resultado del banner en `show banner motd` el comando. Debe leer y seguir estas instrucciones para garantizar la configuración y el funcionamiento correctos del interruptor.

Muestra el ejemplo

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Storage.txt
* Date       : 10-23-2020
* Version    : v1.6
*
* Port Usage : Storage configuration
* Ports 1-36: 100GbE Controller and Shelf Storage Ports
*****
*****
```

5. Compruebe que el 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.

6. Registre cualquier adición personalizada entre la actual `running-config` archivo y el archivo RCF en uso.
7. Después de verificar que las versiones de RCF y las configuraciones de los conmutadores sean correctas, copie el archivo `running-config` archivo al `startup-config` archivo.

```
cs1# copy running-config startup-config
[#####] 100% Copy complete
```

8. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.


```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) Para más detalles.

10. Verificar que el write_erase.cfg El archivo se completa como se esperaba:

```
show file bootflash:write_erase.cfg
```

11. Emitir el write erase Comando para borrar la configuración guardada actual:

```
cs1# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

12. Copie la configuración básica guardada anteriormente en la configuración de inicio.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

13. Reinicie el interruptor CS1.

```
cs1# reload

This command will reboot the system. (y/n)? [n] y
```

14. Repita los pasos 1 al 13 en el interruptor cs2.

15. Conecte los puertos de clúster de todos los nodos del clúster de ONTAP a los switches CS1 y CS2.

Paso 2: Verifique las conexiones del interruptor

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
show interface brief
```

Muestra el ejemplo

```
cs1# show interface brief | grep up
mgmt0  --          up      <mgmt ip address>
1000    1500
Eth1/11      1      eth  trunk  up      none
100G(D)  --
Eth1/12      1      eth  trunk  up      none
100G(D)  --
Eth1/13      1      eth  trunk  up      none
100G(D)  --
Eth1/14      1      eth  trunk  up      none
100G(D)  --
Eth1/15      1      eth  trunk  up      none
100G(D)  --
Eth1/16      1      eth  trunk  up      none
100G(D)  --
Eth1/17      1      eth  trunk  up      none
100G(D)  --
Eth1/18      1      eth  trunk  up      none
100G(D)  --
Eth1/23      1      eth  trunk  up      none
100G(D)  --
Eth1/24      1      eth  trunk  up      none
100G(D)  --
Eth1/25      1      eth  trunk  up      none
100G(D)  --
Eth1/26      1      eth  trunk  up      none
100G(D)  --
Eth1/27      1      eth  trunk  up      none
100G(D)  --
Eth1/28      1      eth  trunk  up      none
100G(D)  --
Eth1/29      1      eth  trunk  up      none
100G(D)  --
Eth1/30      1      eth  trunk  up      none
100G(D)  --
```

2. Compruebe que los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Po999
30	VLAN0030	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9, Eth1/10, Eth1/11 Eth1/12, Eth1/13, Eth1/14 Eth1/15, Eth1/16, Eth1/17 Eth1/18, Eth1/19, Eth1/20 Eth1/21, Eth1/22, Eth1/23 Eth1/24, Eth1/25, Eth1/26 Eth1/27, Eth1/28, Eth1/29 Eth1/30, Eth1/31, Eth1/32 Eth1/33, Eth1/34, Eth1/35 Eth1/36

```
cs1# show interface trunk
```

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--

Eth1/9	1	trunking	--
Eth1/10	1	trunking	--
Eth1/11	1	trunking	--
Eth1/12	1	trunking	--
Eth1/13	1	trunking	--
Eth1/14	1	trunking	--
Eth1/15	1	trunking	--
Eth1/16	1	trunking	--
Eth1/17	1	trunking	--
Eth1/18	1	trunking	--
Eth1/19	1	trunking	--
Eth1/20	1	trunking	--
Eth1/21	1	trunking	--
Eth1/22	1	trunking	--
Eth1/23	1	trunking	--
Eth1/24	1	trunking	--
Eth1/25	1	trunking	--
Eth1/26	1	trunking	--
Eth1/27	1	trunking	--
Eth1/28	1	trunking	--
Eth1/29	1	trunking	--
Eth1/30	1	trunking	--
Eth1/31	1	trunking	--
Eth1/32	1	trunking	--
Eth1/33	1	trunking	--
Eth1/34	1	trunking	--
Eth1/35	1	trunking	--
Eth1/36	1	trunking	--

Port	Vlans Allowed on Trunk

Eth1/1	30
Eth1/2	30
Eth1/3	30
Eth1/4	30
Eth1/5	30
Eth1/6	30
Eth1/7	30
Eth1/8	30
Eth1/9	30
Eth1/10	30
Eth1/11	30
Eth1/12	30

Eth1/13	30
Eth1/14	30
Eth1/15	30
Eth1/16	30
Eth1/17	30
Eth1/18	30
Eth1/19	30
Eth1/20	30
Eth1/21	30
Eth1/22	30
Eth1/23	30
Eth1/24	30
Eth1/25	30
Eth1/26	30
Eth1/27	30
Eth1/28	30
Eth1/29	30
Eth1/30	30
Eth1/31	30
Eth1/32	30
Eth1/33	30
Eth1/34	30
Eth1/35	30
Eth1/36	30

Port	Vlans Err-disabled on Trunk

Eth1/1	none
Eth1/2	none
Eth1/3	none
Eth1/4	none
Eth1/5	none
Eth1/6	none
Eth1/7	none
Eth1/8	none
Eth1/9	none
Eth1/10	none
Eth1/11	none
Eth1/12	none
Eth1/13	none
Eth1/14	none
Eth1/15	none
Eth1/16	none

Eth1/17	none
Eth1/18	none
Eth1/19	none
Eth1/20	none
Eth1/21	none
Eth1/22	none
Eth1/23	none
Eth1/24	none
Eth1/25	none
Eth1/26	none
Eth1/27	none
Eth1/28	none
Eth1/29	none
Eth1/30	none
Eth1/31	none
Eth1/32	none
Eth1/33	none
Eth1/34	none
Eth1/35	none
Eth1/36	none

Port	STP Forwarding

Eth1/1	none
Eth1/2	none
Eth1/3	none
Eth1/4	none
Eth1/5	none
Eth1/6	none
Eth1/7	none
Eth1/8	none
Eth1/9	none
Eth1/10	none
Eth1/11	30
Eth1/12	30
Eth1/13	30
Eth1/14	30
Eth1/15	30
Eth1/16	30
Eth1/17	30
Eth1/18	30
Eth1/19	none
Eth1/20	none

Eth1/21	none
Eth1/22	none
Eth1/23	30
Eth1/24	30
Eth1/25	30
Eth1/26	30
Eth1/27	30
Eth1/28	30
Eth1/29	30
Eth1/30	30
Eth1/31	none
Eth1/32	none
Eth1/33	none
Eth1/34	none
Eth1/35	none
Eth1/36	none

 Port Vlans in spanning tree forwarding state and not pruned

Eth1/1	Feature VTP is not enabled
none	
Eth1/2	Feature VTP is not enabled
none	
Eth1/3	Feature VTP is not enabled
none	
Eth1/4	Feature VTP is not enabled
none	
Eth1/5	Feature VTP is not enabled
none	
Eth1/6	Feature VTP is not enabled
none	
Eth1/7	Feature VTP is not enabled
none	
Eth1/8	Feature VTP is not enabled
none	
Eth1/9	Feature VTP is not enabled
none	
Eth1/10	Feature VTP is not enabled
none	
Eth1/11	Feature VTP is not enabled
30	
Eth1/12	Feature VTP is not enabled
30	

Eth1/13	Feature VTP is not enabled
30	
Eth1/14	Feature VTP is not enabled
30	
Eth1/15	Feature VTP is not enabled
30	
Eth1/16	Feature VTP is not enabled
30	
Eth1/17	Feature VTP is not enabled
30	
Eth1/18	Feature VTP is not enabled
30	
Eth1/19	Feature VTP is not enabled
none	
Eth1/20	Feature VTP is not enabled
none	
Eth1/21	Feature VTP is not enabled
none	
Eth1/22	Feature VTP is not enabled
none	
Eth1/23	Feature VTP is not enabled
30	
Eth1/24	Feature VTP is not enabled
30	
Eth1/25	Feature VTP is not enabled
30	
Eth1/26	Feature VTP is not enabled
30	
Eth1/27	Feature VTP is not enabled
30	
Eth1/28	Feature VTP is not enabled
30	
Eth1/29	Feature VTP is not enabled
30	
Eth1/30	Feature VTP is not enabled
30	
Eth1/31	Feature VTP is not enabled
none	
Eth1/32	Feature VTP is not enabled
none	
Eth1/33	Feature VTP is not enabled
none	
Eth1/34	Feature VTP is not enabled
none	
Eth1/35	Feature VTP is not enabled
none	


```
Eth1/36      Feature VTP is not enabled
none
```



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

Paso 3: Configure el cluster ONTAP

NetApp recomienda usar System Manager para configurar clústeres nuevos.

System Manager proporciona un flujo de trabajo sencillo y sencillo para la instalación y la configuración del clúster, incluidas la asignación de una dirección IP de gestión de nodos, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento del almacenamiento inicial.

Vaya a. ["Configure ONTAP en un nuevo clúster con System Manager"](#) para obtener instrucciones de configuración.

El futuro

Después de haber instalado o actualizado su RCF, ["verificar la configuración de SSH"](#)

Compruebe su configuración SSH

Si utiliza la supervisión de estado del switch Ethernet (CSHM) y las funciones de recogida de registros, compruebe que las claves SSH y SSH estén habilitadas en los switches de clústeres.

Pasos

1. Compruebe que SSH está habilitado:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Compruebe que las claves SSH estén habilitadas:

```
show ssh key
```

Muestra el ejemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yIPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDsrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(switch)# show feature | include scpServer
scpServer          1          enabled
(switch)# show feature | include ssh
sshServer          1          enabled
(switch)#
```



Al habilitar FIPS, debe cambiar el bitcount a 256 en el conmutador mediante el comando `ssh key ecdsa 256 force`. Consulte ["Configurar la seguridad de red con FIPS"](#) para obtener más información.

El futuro

Después de haber verificado su configuración SSH, ["configurar la monitorización del estado del conmutador"](#).

Restablecer los conmutadores de almacenamiento 9336C-FX2 y 9336C-FX2-T a los valores predeterminados de fábrica

Para restablecer los interruptores de almacenamiento 9336C-FX2 y 9336C-FX2-T a los valores predeterminados de fábrica, debe borrar las configuraciones de los interruptores 9336C-FX2 y 9336C-FX2-T.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Borrar la configuración existente:

```
write erase
```

```
(cs2)# write erase
```

```
Warning: This command will erase the startup-configuration.  
Do you wish to proceed anyway? (y/n) [n] y
```

2. Recargue el software del conmutador:

```
reload
```

```
(cs2)# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

El sistema se reinicia y entra en el asistente de configuración. Durante el arranque, si recibe el mensaje “¿Desea cancelar el aprovisionamiento automático y continuar con la configuración normal?” (sí/no)[n]”, debe responder **sí** para continuar.

Reemplace los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T

Puede reemplazar los conmutadores Nexus 9336C-FX2 y 9336C-FX2-T defectuosos en una red de clúster. Este es un procedimiento que no produce interrupciones.

Antes de empezar

Antes de instalar el software NX-OS y los RCF en los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T, asegúrese de lo siguiente:

- Su sistema puede admitir los conmutadores de almacenamiento Cisco Nexus 9336C-FX2 y 9336C-FX2-T.
- Ha consultado la tabla de compatibilidad de switches de la página Cisco Ethernet Switch para ver las versiones ONTAP, NX-OS y RCF compatibles.

- Ha hecho referencia a las guías de software y actualización adecuadas disponibles en el sitio web de Cisco.

Switches Cisco Nexus serie 3000:

- Ha descargado los RCF correspondientes.
- La configuración de red existente tiene 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.
- El switch Cisco Nexus 9336C-FX2 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 configuración inicial del interruptor.

Acerca de esta tarea

Este procedimiento sustituye al segundo switch de almacenamiento Nexus 9336C-FX2 S2 con el nuevo switch 9336C-FX NS2. Los dos nodos son 1 y 2.

Pasos a completar:

- Confirmar que el interruptor que se va a sustituir es S2.
- Desconectar los cables del interruptor S2.
- Vuelva a conectar los cables al conmutador NS2.
- Verifique todas las configuraciones del dispositivo en el conmutador NS2.



Puede haber dependencias entre la sintaxis de comandos en las versiones RCF y NX-OS.

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
```

x es la duración de la ventana de mantenimiento en horas.

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 (Gb/s)	State	Status	VLAN ID

node1	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

```
storage::*>
```

3. Verifique que el interruptor de almacenamiento S1 esté disponible:

```
network device-discovery show
```

Muestra el ejemplo

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol   Port  Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
          e3a   S1                        Ethernet1/1 NX9336C
          e4a   node2                    e4a         AFF-A700
          e4e   node2                    e4e         AFF-A700
node1/lldp
          e3a   S1                        Ethernet1/1 -
          e4a   node2                    e4a         -
          e4e   node2                    e4e         -
node2/cdp
          e3a   S1                        Ethernet1/2 NX9336C
          e4a   node1                    e4a         AFF-A700
          e4e   node1                    e4e         AFF-A700
node2/lldp
          e3a   S1                        Ethernet1/2 -
          e4a   node1                    e4a         -
          e4e   node1                    e4e         -
storage::*>
```

4. Ejecute el programa `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
```

5. 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  -           -  
3.20     2  Ethernet1/6  S1  
3.20     3  -           -  
3.30     0  Ethernet1/7  S1  
3.20     1  -           -  
3.30     2  Ethernet1/8  S1  
3.20     3  -           -  
storage::*>
```

6. Retire todos los cables conectados al interruptor de almacenamiento S2.

7. Vuelva a conectar todos los cables al interruptor de sustitución NS2.

8. Vuelva a comprobar 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  
  
Node           Port Type  Mode    Speed      State   Status   VLAN  
-----  ----  ----  -  
node1  
          e3a  ENET  storage 100    enabled  online   30  
          e3b  ENET  storage 0      enabled  offline  30  
          e7a  ENET  storage 0      enabled  offline  30  
          e7b  ENET  storage 0      enabled  offline  30  
node2  
          e3a  ENET  storage 100    enabled  online   30  
          e3b  ENET  storage 0      enabled  offline  30  
          e7a  ENET  storage 0      enabled  offline  30  
          e7b  ENET  storage 0      enabled  offline  30  
storage::*>
```

9. Compruebe que ambos conmutadores estén disponibles:

```
network device-discovery show
```

Muestra el ejemplo

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e3a  S1                        Ethernet1/1 NX9336C
          e4a  node2                    e4a         AFF-A700
          e4e  node2                    e4e         AFF-A700
          e7b  NS2                     Ethernet1/1 NX9336C
node1/lldp
          e3a  S1                        Ethernet1/1 -
          e4a  node2                    e4a         -
          e4e  node2                    e4e         -
          e7b  NS2                     Ethernet1/1 -
node2/cdp
          e3a  S1                        Ethernet1/2 NX9336C
          e4a  node1                    e4a         AFF-A700
          e4e  node1                    e4e         AFF-A700
          e7b  NS2                     Ethernet1/2 NX9336C
node2/lldp
          e3a  S1                        Ethernet1/2 -
          e4a  node1                    e4a         -
          e4e  node1                    e4e         -
          e7b  NS2                     Ethernet1/2 -
storage::*>
```

10. 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  
storage::*>
```

11. 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
```

El futuro

Después de haber reemplazado los interruptores, ["configurar la monitorización del estado del conmutador"](#).

NVIDIA SN2100

Manos a la obra

Flujo de trabajo de instalación y configuración para conmutadores NVIDIA SN2100

El NVIDIA SN2100 es un switch Ethernet que le permite cambiar datos entre controladoras y bandejas de discos.

Siga estos pasos de flujo de trabajo para instalar y configurar sus conmutadores SN2100.

1

"Revisar los requisitos de configuración"

Revise los requisitos de configuración para el conmutador de almacenamiento SN2100.

2

"Revise los componentes y números de pieza"

Revise los componentes y números de pieza del conmutador de almacenamiento SN2100.

3

"Revisar la documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores SN2100 y el clúster ONTAP .



"Instale el hardware"

Instale el hardware del interruptor.



"Configurar el software"

Configurar el software del conmutador.

Requisitos de configuración para los switches NVIDIA SN2100

Para la instalación y el mantenimiento del conmutador NVIDIA SN2100, asegúrese de revisar todos los requisitos.

Requisitos de instalación

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.

El conmutador NVIDIA SN2100 (X190006/X190106) se instala en el armario de conmutadores doble/único NVIDIA con los soportes estándar que se incluyen con el conmutador.

Para conocer las pautas de cableado, consulte ["Consideraciones sobre el cableado y la configuración"](#) .

Soporte de ONTAP y Linux

El conmutador NVIDIA SN2100 es un conmutador Ethernet de 10/25/40/100 GB que ejecuta Cumulus Linux. El conmutador admite lo siguiente:

- ONTAP 9.10.1P3. El switch SN2100 sirve a las aplicaciones de clúster y almacenamiento de ONTAP 9.10.1P3 sobre diferentes pares de switches. Desde ONTAP 9.10.1P3, puede utilizar los switches NVIDIA SN2100 para combinar las funciones de almacenamiento y clúster en una configuración de switch compartido.
- Cumulus Linux (CL) OS versión 4.4.3. Para obtener información actual sobre compatibilidad, consulte ["Switches Ethernet de NVIDIA"](#) página de información.
- Puede instalar Cumulus Linux cuando el conmutador esté ejecutando Cumulus Linux o ONIE.

¿Qué sigue?

["Componentes y números de pieza"](#) .

Componentes y números de pieza para conmutadores NVIDIA SN2100

Para la instalación y el mantenimiento del switch NVIDIA SN2100, asegúrese de revisar la lista de componentes y números de pieza para el kit de armarios y rieles.

Detalles del armario

El conmutador NVIDIA SN2100 (X190006/X190106) se instala en el armario de conmutadores doble/único NVIDIA con los soportes estándar que se incluyen con el conmutador.

Detalles del kit de rieles

La tabla siguiente muestra el número de pieza y la descripción de los interruptores y kits de raíles MSN2100:

Número de pieza	Descripción
X190006-PE	Cluster Switch, NVIDIA SN2100, 16PT 100G, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16PT 100G, PSIN
X190106-FE-PE	Conmutador, NVIDIA SN2100, 16PT 100G, PTSX, front-end
X190106-FE-PI	Conmutador, NVIDIA SN2100, 16PT 100G, PSIN, front-end
X-MTEF-KIT-D	Kit de rieles, conmutador doble NVIDIA lado a lado
X-MTEF-KIT-E	Kit de rieles, profundidad corta de un único conmutador NVIDIA



Consulte la documentación de NVIDIA para obtener más información acerca de ["Instalación del kit de rieles y interruptor SN2100"](#).

¿Qué sigue?

["Documentación requerida"](#) .

Requisitos de documentación para los switches NVIDIA SN2100

Para la instalación y el mantenimiento del conmutador NVIDIA SN2100, asegúrese de revisar toda la documentación recomendada.

En la siguiente tabla se muestra la documentación disponible para los conmutadores NVIDIA SN2100.

Título	Descripción
"Configurar y configurar los switches NVIDIA SN2100"	Describe cómo configurar y configurar los conmutadores NVIDIA SN2100, incluida la instalación de Cumulus Linux y RCF aplicables.
"Migrar de un conmutador de almacenamiento Cisco a un conmutador de almacenamiento NVIDIA SN2100"	Describe cómo migrar desde entornos que utilizan conmutadores de almacenamiento Cisco a entornos que utilizan conmutadores de almacenamiento NVIDIA SN2100.
"Migre a un clúster con switches de dos nodos con switches de clúster NVIDIA SN2100"	Describe cómo migrar a un entorno con switches de dos nodos mediante switches de clúster NVIDIA SN2100.
"Reemplace un conmutador de almacenamiento NVIDIA SN2100"	Describe el procedimiento para sustituir un conmutador de almacenamiento NVIDIA SN2100 defectuoso y descargar Cumulus Linux y el archivo de configuración de referencia.

Instale el hardware

Flujo de trabajo de instalación de hardware para conmutadores de almacenamiento NVIDIA SN2100

Para instalar y configurar el hardware de un conmutador de almacenamiento SN2100, siga estos pasos:

1

"Instale el hardware"

Instale el hardware del interruptor.

2

"Revise las consideraciones sobre el cableado y la configuración"

Revise los requisitos para las conexiones ópticas, el adaptador QSA y la velocidad del puerto de conmutación.

3

"Conecte el cable de las bandejas NS224"

Siga los procedimientos de cableado si dispone de un sistema en el que las bandejas de unidades NS224 deban cablearse como almacenamiento conectado a switch (no como almacenamiento de conexión directa).

Instale la tornillería del conmutador NVIDIA SN2100

Para instalar el hardware SN2100, consulte la documentación de NVIDIA.

Pasos

1. Revise la "requisitos de configuración".
2. Siga las instrucciones de "Guía de instalación del switch NVIDIA".

El futuro

"Revisar el cableado y la configuración" .

Revise las consideraciones sobre el cableado y la configuración

Antes de configurar el conmutador NVIDIA SN2100, revise las siguientes consideraciones.

Detalles del puerto NVIDIA

Puertos del conmutador	Uso de puertos
swp1s0-3	4 nodos de puertos de clúster de 10 GbE de arranque
swp2s0-3	4 nodos de puertos de clúster de 10 GbE de cable abierto
swp3-14	Nodos de puertos de clúster 40/100GbE

swp15-16	100GbE puertos de enlace entre switches (ISL)

Consulte "[Hardware Universe](#)" para obtener más información sobre los puertos de switch.

Retrasos de conexión con conexiones ópticas

Si experimenta retrasos de enlace de más de cinco segundos, Cumulus Linux 5,4 y posterior incluye soporte para conexión rápida. Puede configurar los enlaces mediante `nv set` comando de la siguiente manera:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Muestra el ejemplo

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Soporte para conexiones de cobre

Se requieren los siguientes cambios de configuración para solucionar este problema.

Cumulus Linux 4.4.3

1. Identifique el nombre de cada interfaz mediante cables de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
```

Interface Vendor Rev	Identifier	Vendor Name	Vendor PN	Vendor SN
swp3 B0	0x11 (QSFP28)	Molex	112-00576	93A2229911111
swp4 B0	0x11 (QSFP28)	Molex	112-00576	93A2229922222

2. Añada las dos líneas siguientes a la `/etc/cumulus/switchd.conf` Archivo para cada puerto (swp<n>) que utilice cables de cobre 40GbE/100GbE:

- `interface.swp<n>.enable_media_depended_linkup_flow=TRUE`
- `interface.swp<n>.enable_short_tuning=TRUE`

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
.
.
interface.swp3.enable_media_depended_linkup_flow=TRUE
interface.swp3.enable_short_tuning=TRUE
interface.swp4.enable_media_depended_linkup_flow=TRUE
interface.swp4.enable_short_tuning=TRUE
```

3. Reinicie el `switchd` servicio:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Confirme que los puertos están activos:

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp3	100G	9216	Trunk/L2		Master: bridge(UP)
UP	swp4	100G	9216	Trunk/L2		Master: bridge(UP)

Cumulus Linux 5.x

1. Identifique el nombre de cada interfaz mediante cables de cobre 40GbE/100GbE:

```
cumulus@cumulus:mgmt:~$ nv show interface pluggables
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor SN
Vendor Rev				
swp3	0x11 (QSFP28)	Molex	112-00576	93A2229911111
B0				
swp4	0x11 (QSFP28)	Molex	112-00576	93A2229922222
B0				

2. Configure los enlaces mediante `nv set` comando de la siguiente manera:

- ° `nv set interface <interface-id> link fast-linkup on`
- ° `nv config apply`
- ° Vuelva a cargar el `switchd` servicio

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

3. Confirme que los puertos están activos:

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
UP	swp3	100G	9216	Trunk/L2		Master:
bridge (UP)						
UP	swp4	100G	9216	Trunk/L2		Master:
bridge (UP)						

Consulte el artículo de la base de conocimientos ["El switch SN2100 no se puede conectar mediante cables de cobre de 40/100GbE"](#) para obtener más información.

En Cumulus Linux 4.4.2, las conexiones de cobre no son compatibles con los switches SN2100 con X1151A NIC, X1146A NIC o 100GbE puertos integrados. Por ejemplo:

- AFF A800 en los puertos e0a y e0b
- AFF A320 en los puertos e0g y e0h

Adaptador QSA

Cuando se utiliza un adaptador QSA para conectarse a los puertos de clúster 10GbE/25GbE en una plataforma, es posible que el enlace no aparezca.

Para resolver este problema, haga lo siguiente:

- Para 10GbE, ajuste manualmente la velocidad de enlace swp1s0-3 a 10000 y establezca la negociación automática en OFF.
- Para 25GbE, ajuste manualmente la velocidad de enlace swp2s0-3 a 25000 y establezca la negociación automática en OFF.



Cuando utilice adaptadores QSA de 10GbE/25GbE, insértelos en puertos 40GbE/100GbE que no sean separables (swp3-swp14). No inserte el adaptador QSA en un puerto configurado para la desconexión.

Defina la velocidad de la interfaz en los puertos de conexión

Dependiendo del transceptor en el puerto del switch, es posible que necesite configurar la velocidad en la interfaz del switch a una velocidad fija. Si utiliza puertos de desconexión 10GbE y 25GbE, verifique que la negociación automática esté desactivada y establezca la velocidad de la interfaz en el switch.

Cumulus Linux 4.4.3

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces      2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp1s3
iface swp1s3
    alias 10G Intra-Cluster Node
-   link-autoneg off
+   link-autoneg on
    link-speed 10000 <---- port speed set
    mstpctl-bpduguard yes
    mstpctl-portadminedge yes
    mtu 9216

auto swp2s0
iface swp2s0
    alias 25G Intra-Cluster Node
    link-autoneg off
    link-speed 25000 <---- port speed set
```

Compruebe el estado de la interfaz y del puerto para verificar que se aplican los ajustes:

```
cumulus@cumulus:mgmt:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	

.						
.						
UP	swp1s0	10G	9216	Trunk/L2	cs07 (e4c)	Master:
br_default(UP)						
UP	swp1s1	10G	9216	Trunk/L2	cs07 (e4d)	Master:
br_default(UP)						
UP	swp1s2	10G	9216	Trunk/L2	cs08 (e4c)	Master:
br_default(UP)						
UP	swp1s3	10G	9216	Trunk/L2	cs08 (e4d)	Master:
br_default(UP)						
.						
.						
UP	swp3	40G	9216	Trunk/L2	cs03 (e4e)	Master:
br_default(UP)						
UP	swp4	40G	9216	Trunk/L2	cs04 (e4e)	Master:
br_default(UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
br_default(UP)						
.						
.						
UP	swp15	100G	9216	BondMember	cs01 (swp15)	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	cs01 (swp16)	Master:
cluster_isl(UP)						
.						
.						

Cumulus Linux 5.x

Por ejemplo:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3
```

```
link
```

auto-negotiate	off	off
duplex	full	full
speed	10G	10G
fec	auto	auto
mtu	9216	9216
[breakout]		
state	up	up

Compruebe el estado de la interfaz y del puerto para verificar que se aplican los ajustes:

```
cumulus@cumulus:mgmt:~$ nv show interface
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	
.						
.						
UP	swp1s0	10G	9216	Trunk/L2	cs07 (e4c)	Master:
br_default(UP)						
UP	swp1s1	10G	9216	Trunk/L2	cs07 (e4d)	Master:
br_default(UP)						
UP	swp1s2	10G	9216	Trunk/L2	cs08 (e4c)	Master:
br_default(UP)						
UP	swp1s3	10G	9216	Trunk/L2	cs08 (e4d)	Master:
br_default(UP)						
.						
.						
UP	swp3	40G	9216	Trunk/L2	cs03 (e4e)	Master:
br_default(UP)						
UP	swp4	40G	9216	Trunk/L2	cs04 (e4e)	Master:
br_default(UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
br_default(UP)						
.						
.						
UP	swp15	100G	9216	BondMember	cs01 (swp15)	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	cs01 (swp16)	Master:
cluster_isl(UP)						
.						
.						

El futuro

"Conecte el cable de las bandejas NS224 como almacenamiento conectado al conmutador".

Conecte el cable de las bandejas NS224 como almacenamiento conectado al conmutador

Si tiene un sistema en el que las bandejas de unidades NS224 deben cablearse como almacenamiento conectado al switch (no como almacenamiento de conexión directa), utilice la información proporcionada aquí.

- Conectar las bandejas de unidades NS224 a través de switches de almacenamiento:

["Información para cableado de bandejas de unidades NS224 conectadas a switch"](#)

- Instale los switches de almacenamiento:

["Documentación de AFF y switches FAS"](#)

- Confirme el hardware compatible, como los switches y cables de almacenamiento, para su modelo de plataforma:

["Hardware Universe de NetApp"](#)

Configurar el software

Flujo de trabajo de instalación de software para los switches de almacenamiento NVIDIA SN2100

Para instalar y configurar el software para un conmutador NVIDIA SN2100, siga estos pasos:

1

["Configure el switch"](#)

Configurar el conmutador NVIDIA SN2100.

2

["Instale Cumulus Linux en modo Cumulus"](#)

Puede instalar el sistema operativo Cumulus Linux (CL) cuando el conmutador ejecuta Cumulus Linux.

3

["Instale Cumulus Linux en modo ONIE"](#)

Como alternativa, puede instalar el sistema operativo Cumulus Linux (CL) cuando el conmutador ejecuta Cumulus Linux en modo ONIE.

4

["Instale la secuencia de comandos del archivo de configuración de referencia \(RCF\)"](#)

Hay dos secuencias de comandos RCF disponibles para las aplicaciones de almacenamiento y agrupación en clúster. El procedimiento para cada uno es el mismo.

5

["Instale el archivo CSHM"](#)

Puede instalar el archivo de configuración correspondiente para la supervisión del estado del switch Ethernet de los switches de clúster de NVIDIA.

6

["Restablecer el interruptor a los valores predeterminados de fábrica"](#)

Borre la configuración del interruptor de almacenamiento SN2100.

Configure el conmutador NVIDIA SN2100

Para configurar el conmutador SN2100, consulte la documentación de NVIDIA.

Pasos

1. Revise la ["requisitos de configuración"](#).
2. Siga las instrucciones de ["Puesta en marcha del sistema NVIDIA."](#)

El futuro

["Instale Cumulus Linux en modo Cumulus"](#) o ["Instale Cumulus Linux en modo ONIE"](#).

Instale Cumulus Linux en modo Cumulus

Siga este procedimiento para instalar Cumulus Linux (CL) OS cuando el conmutador se esté ejecutando en modo Cumulus.



Cumulus Linux (CL) OS se puede instalar ya sea cuando el conmutador ejecuta Cumulus Linux o ONIE (consulte ["Instale EN modo ONIE"](#)).

Antes de empezar

Asegúrese de que esté disponible lo siguiente:

- Conocimientos de Linux de nivel intermedio.
- Estar familiarizado con la edición de texto básica, los permisos de archivos UNIX y la supervisión de procesos. Una variedad de editores de texto están preinstalados, incluyendo `vi` y `nano`.
- Acceso a un shell de Linux o UNIX. Si ejecuta Windows, utilice un entorno Linux como herramienta de línea de comandos para interactuar con Cumulus Linux.
- El requisito de velocidad en baudios debe establecerse en 115200 en el conmutador de consola serie para el acceso a la consola del conmutador NVIDIA SN2100, como se indica a continuación:
 - 115200 baudios
 - 8 bits de datos
 - 1 bit de parada
 - paridad: none
 - control de flujo: ninguno

Acerca de esta tarea

Tenga en cuenta lo siguiente:



Cada vez que se instala Cumulus Linux, se borra y reconstruye toda la estructura del sistema de archivos.



La contraseña predeterminada para la cuenta de usuario de cumulus es **cumulus**. La primera vez que inicie sesión en Cumulus Linux, debe cambiar esta contraseña predeterminada. Asegúrese de actualizar cualquier secuencia de comandos de automatización antes de instalar una nueva imagen. Cumulus Linux proporciona opciones de línea de comandos para cambiar automáticamente la contraseña predeterminada durante el proceso de instalación.

Ejemplo 6. Pasos

Cumulus Linux 4.4.3

1. Inicie sesión en el switch.

La primera vez que inicia sesión en el conmutador requiere nombre de usuario/contraseña de **cumulus/cumulus** con sudo privilegios.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Compruebe la versión de Cumulus Linux: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo se inicia después de reiniciar la sesión de la consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz se utiliza específicamente para la gestión fuera de banda. De forma predeterminada, la interfaz de gestión utiliza DHCPv4 para la direccionamiento.



No utilice caracteres de subrayado (_), apóstrofe (') o no ASCII en el nombre de host.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Este comando modifica ambos `/etc/hostname` y `/etc/hosts` archivos.

4. Confirme que se han actualizado el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Establezca la fecha, la hora, la zona horaria y el servidor NTP en el switch.

- a. Compruebe la zona horaria actual:

```
cumulus@sw1:~$ cat /etc/timezone
```

- b. Actualizar a la nueva zona horaria:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```


c. Verifique su zona horaria actual:

```
cumulus@switch:~$ date +%Z
```

d. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Ajuste el reloj del software según la zona horaria configurada:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Ajuste el valor actual del reloj del software en el reloj del hardware:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>  
iburst  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

h. Compruebe que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp  
ntp          4074      1   0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p  
/var/run/ntpd.pid -g -u 101:102
```

i. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que usa NTP es eth0. Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ net add time ntp source <src_int>  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

6. Instale Cumulus Linux 4.4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el conmutador NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones de pantalla de GRUB. * No* realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar el sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Compruebe que la versión de Cumulus Linux es 4.4.3: `net show version`

```
cumulus@sw1:mgmt:~$ net show version  
NCLU_VERSION=1.0-cl4.4.3u0  
DISTRIB_ID="Cumulus Linux"  
DISTRIB_RELEASE=4.4.3  
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Cree un nuevo usuario y agregue este usuario a `sudo` grupo. Este usuario sólo se hace efectivo después de reiniciar la sesión de la consola/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

Cumulus Linux 5.4.0

1. Inicie sesión en el switch.

La primera vez que inicia sesión en el conmutador requiere nombre de usuario/contraseña de

cumulus/cumulus con sudo privilegios.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Compruebe la versión de Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.3.0	system build version
uptime	6 days, 8:37:36	system uptime
timezone	Etc/UTC	system time zone

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo se inicia después de reiniciar la sesión de la consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz se utiliza específicamente para la gestión fuera de banda. De forma predeterminada, la interfaz de gestión utiliza DHCPv4 para la direccionamiento.



No utilice caracteres de subrayado (`_`), apóstrofe (`'`) o no ASCII en el nombre de host.

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica ambos `/etc/hostname` y `/etc/hosts` archivos.

4. Confirme que se han actualizado el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

```

cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1

```

5. Establezca la zona horaria, la fecha, la hora y el servidor NTP en el switch.

a. Establezca la zona horaria:

```

cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply

```

b. Verifique su zona horaria actual:

```

cumulus@switch:~$ date +%Z

```

c. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```

cumulus@sw1:~$ sudo dpkg-reconfigure tzdata

```

d. Ajuste el reloj del software según la zona horaria configurada:

```

cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"

```

e. Ajuste el valor actual del reloj del software en el reloj del hardware:

```

cumulus@sw1:~$ sudo hwclock -w

```

f. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Consulte el artículo de la base de conocimientos "[La configuración del servidor NTP no funciona con los conmutadores NVIDIA SN2100](#)" Para más detalles.

g. Compruebe que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp          4074      1   0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que usa NTP es eth0. Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instale Cumulus Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el conmutador NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones de pantalla de GRUB. * No* realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar el sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Compruebe que la versión de Cumulus Linux es 5.4.0: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	system build version
uptime	6 days, 13:37:36	system uptime
timezone	Etc/UTC	system time zone

11. Compruebe que cada nodo tenga una conexión con cada switch:

```
cumulus@sw1:mgmt:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost
RemotePort			
eth0	100M	Mgmt	mgmt-sw1
Eth110/1/29			
swp2s1	25G	Trunk/L2	node1
e0a			
swp15	100G	BondMember	sw2
swp15			
swp16	100G	BondMember	sw2
swp16			

12. Cree un nuevo usuario y agregue este usuario a sudo grupo. Este usuario sólo se hace efectivo después de reiniciar la sesión de la consola/SSH.

```
sudo adduser --ingroup netedit admin
```

```

cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$

```

13. Agregue grupos de usuarios adicionales al que pueda acceder el usuario administrador `nv` comandos:


```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user 'admin' to group 'nvshow' ...
Adding user admin to group nvshow
Done.
```

Consulte ["Cuentas de usuario de NVIDIA"](#) si quiere más información.

Cumulus Linux 5.11.0

1. Inicie sesión en el switch.

Cuando inicia sesión en el conmutador por primera vez, requiere el nombre de usuario/contraseña de **cumulus/cumulus** con sudo Privileges.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Compruebe la versión de Cumulus Linux: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	system build version
uptime	6 days, 8:37:36	system uptime
timezone	Etc/UTC	system time zone

3. Configure el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada. El nuevo nombre de host solo se inicia después de reiniciar la sesión de la consola/SSH.



Un switch Cumulus Linux proporciona al menos un puerto de administración Ethernet dedicado llamado `eth0`. Esta interfaz se utiliza específicamente para la gestión fuera de banda. De forma predeterminada, la interfaz de gestión utiliza DHCPv4 para la direccionamiento.



No utilice caracteres de subrayado (`_`), apóstrofe (`'`) o no ASCII en el nombre de host.

```
cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Este comando modifica ambos `/etc/hostname` y `/etc/hosts` archivos.

4. Confirme que se han actualizado el nombre de host, la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Establezca la zona horaria, la fecha, la hora y el servidor NTP en el switch.

- a. Establezca la zona horaria:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

- b. Verifique su zona horaria actual:

```
cumulus@switch:~$ date +%Z
```

- c. Para configurar la zona horaria mediante el asistente guiado, ejecute el siguiente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

- d. Ajuste el reloj del software según la zona horaria configurada:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

- e. Ajuste el valor actual del reloj del software en el reloj del hardware:

```
cumulus@sw1:~$ sudo hwclock -w
```

- f. Agregue un servidor NTP si es necesario:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Consulte el artículo de la base de conocimientos ["La configuración del servidor NTP no funciona con los conmutadores NVIDIA SN2100"](#) Para más detalles.

- g. Compruebe que ntpd se está ejecutando en el sistema:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp          4074      1   0 Jun20 ?           00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

- h. Especifique la interfaz de origen NTP. Por defecto, la interfaz de origen que usa NTP es eth0. Puede configurar una interfaz de origen NTP diferente de la siguiente manera:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Instale Cumulus Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

El instalador inicia la descarga. Escriba **y** cuando se le solicite.

7. Reinicie el conmutador NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. La instalación se inicia automáticamente y aparecen las siguientes opciones de pantalla de GRUB. * No* realice ninguna selección.

- Cumulus-Linux GNU/Linux
- ONIE: Instalar el sistema operativo
- CUMULUS-INSTALL
- Cumulus-Linux GNU/Linux

9. Repita los pasos del 1 al 4 para iniciar sesión.

10. Compruebe que la versión de Cumulus Linux es 5.11.0:

```
nv show system
```

```
cumulus@cumulus:mgmt:~$ nv show system
```

operational	applied	description
build	Cumulus Linux 5.11.0	
uptime	153 days, 2:44:16	
hostname	cumulus	cumulus
product-name	Cumulus Linux	
product-release	5.11.0	
platform	x86_64-mlnx_x86-r0	
system-memory	2.76 GB used / 2.28 GB free / 7.47 GB total	
swap-memory	0 Bytes used / 0 Bytes free / 0 Bytes total	
health-status	not OK	
date-time	2025-04-23 09:55:24	
status	N/A	
timezone	Etc/UTC	
maintenance		
mode	disabled	
ports	enabled	
version		
kernel	6.1.0-cl-1-amd64	
build-date	Thu Nov 14 13:06:38 UTC 2024	
image	5.11.0	
onie	2019.11-5.2.0020-115200	

11. Compruebe que cada nodo tenga una conexión con cada switch:

```
cumulus@sw1:mgmt:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost
RemotePort			

eth0	100M	eth	mgmt-sw1
Eth110/1/14			
swp2s1	25G	Trunk/L2	node1
e0a			
swp1s1	10G	swp	sw2
e0a			
swp9	100G	swp	sw3
e4a			
swp10	100G	swp	sw4
e4a			
swp15	100G	swp	sw5
swp15			
swp16	100G	swp	sw6
swp16			

Consulte ["Cuentas de usuario de NVIDIA"](#) para obtener más información.

El futuro

["Instale o actualice el script RCF"](#).

Instale Cumulus Linux en modo ONIE

Siga este procedimiento para instalar Cumulus Linux (CL) OS cuando el conmutador se ejecute EN modo ONIE.



Cumulus Linux (CL) OS se puede instalar ya sea cuando el conmutador ejecuta Cumulus Linux o ONIE (consulte ["Instalar en modo Cumulus"](#)).

Acerca de esta tarea

Puede instalar Cumulus Linux utilizando Open Network Install Environment (ONIE) que permite la detección automática de una imagen del instalador de red. Esto facilita el modelo de sistema de asegurar los conmutadores con una opción de sistema operativo, como Cumulus Linux. La forma más fácil de instalar Cumulus Linux con ONIE es con el descubrimiento HTTP local.



Si el host tiene IPv6 habilitada, asegúrese de que ejecuta un servidor web. Si el host tiene la función IPv4 habilitada, asegúrese de que esté ejecutando DHCP además de un servidor web.

Este procedimiento muestra cómo actualizar Cumulus Linux después de que el administrador haya arrancado EN ONIE.

Pasos

1. Descargue el archivo de instalación de Cumulus Linux en el directorio raíz del servidor Web. Cambie el nombre de este archivo `onie-installer`.
2. Conecte el host al puerto Ethernet de gestión del switch mediante un cable Ethernet.
3. Encienda el interruptor. El conmutador descarga el instalador DE imágenes ONIE y arranca. Una vez finalizada la instalación, aparece el indicador de inicio de sesión de Cumulus Linux en la ventana del terminal.



Cada vez que se instala Cumulus Linux, se borra y reconstruye toda la estructura del sistema de archivos.

4. Reinicie el interruptor SN2100:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

5. Pulse la tecla **Esc** en la pantalla GNU GRUB para interrumpir el proceso de arranque normal, seleccione **ONIE** y pulse **Intro**.
6. En la siguiente pantalla, seleccione **ONIE: Install OS**.
7. EL proceso DE detección DEL instalador DE ONIE ejecuta la búsqueda de la instalación automática. Pulse **Intro** para detener temporalmente el proceso.
8. Cuando el proceso de detección se detuvo:

```
ONIE:/ # onie-stop  
discover: installer mode detected.  
Stopping: discover...start-stop-daemon: warning: killing process 427:  
No such process done.
```

9. Si el servicio DHCP se está ejecutando en la red, compruebe que la dirección IP, la máscara de subred y la puerta de enlace predeterminada están correctamente asignadas:

```
ifconfig eth0
```

Muestra el ejemplo

```
ONIE:/ # ifconfig eth0
eth0    Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
        inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
        inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
Memory:dfc00000-dfc1ffff
```

```
ONIE:/ # route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref
Use Iface

default          10.233.204.1    0.0.0.0          UG    0     0
0 eth0
10.233.204.0     *               255.255.254.0    U     0     0
0 eth0
```

10. Si el esquema de direccionamiento IP se define manualmente, haga lo siguiente:

```
ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1
```

11. Repita el paso 9 para comprobar que la información estática se ha introducido correctamente.

12. Instalar Cumulus Linux:

```
ONIE:/ # route
```

```
Kernel IP routing table
```

```
ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

```
Stopping: discover... done.
```

```
Info: Attempting
```

```
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-4.4.3-mlx-amd64.bin ...
```

```
Connecting to 10.60.132.97 (10.60.132.97:80)
```

```
installer          100% |*|    552M  0:00:00 ETA
```

```
...
```

```
...
```

13. Una vez finalizada la instalación, inicie sesión en el conmutador:

Muestra el ejemplo

```
cumulus login: cumulus
```

```
Password: cumulus
```

```
You are required to change your password immediately (administrator enforced)
```

```
Changing password for cumulus.
```

```
Current password: cumulus
```

```
New password: <new_password>
```

```
Retype new password: <new_password>
```

14. Verifique la versión de Cumulus Linux:

```
net show version
```

Muestra el ejemplo

```
cumulus@cumulus:mgmt:~$ net show version
```

```
NCLU_VERSION=1.0-cl4.4.3u4
```

```
DISTRIB_ID="Cumulus Linux"
```

```
DISTRIB_RELEASE=4.4.3
```

```
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

El futuro

["Instale o actualice el script RCF"](#) .

Instale o actualice el script RCF

Siga este procedimiento para instalar o actualizar el script RCF.

Antes de empezar

Antes de instalar o actualizar la secuencia de comandos RCF, asegúrese de que los siguientes elementos están disponibles en el conmutador:

- Cumulus Linux 4.4.3 está instalado.
- Dirección IP, máscara de subred y puerta de enlace predeterminada definida a través de DHCP o configurado manualmente.

Versiones actuales de la secuencia de comandos RCF

Hay dos secuencias de comandos RCF disponibles para las aplicaciones de almacenamiento y agrupación en clúster. El procedimiento para cada uno es el mismo.

- Agrupación en clúster: **MSN2100-RCF-v1.x-Cluster**
- Almacenamiento: **MSN2100-RCF-v1.x-Almacenamiento**



El siguiente procedimiento de ejemplo muestra cómo descargar y aplicar el script RCF para los switches de clúster.



El resultado de ejemplo de comando utiliza la dirección IP de gestión del switch 10.233.204.71, la máscara de red 255.255.254.0 y la pasarela predeterminada 10.233.204.1.

Pasos

1. Mostrar las interfaces disponibles en el interruptor SN2100:

```
net show interface all
```

Muestra el ejemplo

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	---	-----	-----	-----	-----
-----	-----	---	-----	-----	-----	-----
...						
...						
ADMDN	swp1	N/A	9216	NotConfigured		
ADMDN	swp2	N/A	9216	NotConfigured		
ADMDN	swp3	N/A	9216	NotConfigured		
ADMDN	swp4	N/A	9216	NotConfigured		
ADMDN	swp5	N/A	9216	NotConfigured		
ADMDN	swp6	N/A	9216	NotConfigured		
ADMDN	swp7	N/A	9216	NotConfigure		
ADMDN	swp8	N/A	9216	NotConfigured		
ADMDN	swp9	N/A	9216	NotConfigured		
ADMDN	swp10	N/A	9216	NotConfigured		
ADMDN	swp11	N/A	9216	NotConfigured		
ADMDN	swp12	N/A	9216	NotConfigured		
ADMDN	swp13	N/A	9216	NotConfigured		
ADMDN	swp14	N/A	9216	NotConfigured		
ADMDN	swp15	N/A	9216	NotConfigured		
ADMDN	swp16	N/A	9216	NotConfigured		

2. Copie la secuencia de comandos de la pitón de RCF en el conmutador:

```
admin@sw1:mgmt:~$ pwd
/home/cumulus
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.8-
Cluster
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.8-Cluster          100% 8607    111.2KB/s
00:00
```

3. Aplique el script de pitón de RCF **MSN2100-RCF-v1.8-Cluster**:

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.8-Cluster
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

La secuencia de comandos RCF completa los pasos indicados anteriormente.



Para cualquier problema de script de Python de RCF que no se pueda corregir, póngase en contacto con ["Soporte de NetApp"](#) para obtener ayuda.

4. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.
5. Verificar la configuración tras el reinicio:

```
net show interface all
```

Muestra el ejemplo

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	-----
...						
...						
DN	swp1s0	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp1s1	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp1s2	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp1s3	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp2s0	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp2s1	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp2s2	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp2s3	N/A	9216	Trunk/L2		Master:
bridge (UP)						
UP	swp3	100G	9216	Trunk/L2		Master:
bridge (UP)						
UP	swp4	100G	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp8	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp9	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp10	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp11	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp12	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp13	N/A	9216	Trunk/L2		Master:
bridge (UP)						

```

DN      swp14      N/A    9216    Trunk/L2      Master:
bridge(UP)
UP      swp15      N/A    9216    BondMember    Master:
bond_15_16(UP)
UP      swp16      N/A    9216    BondMember    Master:
bond_15_16(UP)
...
...

```

```
cumulus@cumulus:mgmt:~$ net show roce config
```

```
RoCE mode..... lossless
```

```
Congestion Control:
```

```
Enabled SPs.... 0 2 5
```

```
Mode..... ECN
```

```
Min Threshold.. 150 KB
```

```
Max Threshold.. 1500 KB
```

```
PFC:
```

```
Status..... enabled
```

```
Enabled SPs.... 2 5
```

```
Interfaces..... swp10-16,swp1s0-3,swp2s0-3,swp3-9
```

DSCP	802.1p	switch-priority
-----	-----	-----
0 1 2 3 4 5 6 7	0	0
8 9 10 11 12 13 14 15	1	1
16 17 18 19 20 21 22 23	2	2
24 25 26 27 28 29 30 31	3	3
32 33 34 35 36 37 38 39	4	4
40 41 42 43 44 45 46 47	5	5
48 49 50 51 52 53 54 55	6	6
56 57 58 59 60 61 62 63	7	7

switch-priority	TC	ETS
-----	--	-----
0 1 3 4 6 7	0	DWRR 28%
2	2	DWRR 28%
5	5	DWRR 43%

6. Verifique la información del transceptor en la interfaz:

```
net show interface pluggables
```

Muestra el ejemplo

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
```

Interface	Identifier	Vendor Name	Vendor PN	Vendor SN
Vendor Rev				
swp3	0x11 (QSFP28)	Amphenol	112-00574	
APF20379253516	B0			
swp4	0x11 (QSFP28)	AVAGO	332-00440	AF1815GU05Z
A0				
swp15	0x11 (QSFP28)	Amphenol	112-00573	
APF21109348001	B0			
swp16	0x11 (QSFP28)	Amphenol	112-00573	
APF21109347895	B0			

7. Compruebe que cada nodo tenga una conexión con cada switch:

```
net show lldp
```

Muestra el ejemplo

```
cumulus@cumulus:mgmt:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	sw1	e3a
swp4	100G	Trunk/L2	sw2	e3b
swp15	100G	BondMember	sw13	swp15
swp16	100G	BondMember	sw14	swp16

8. 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: node1

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

Node: node2

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

- a. Compruebe el estado del switch del clúster (es posible que esto no muestre el switch sw2, ya que las LIF no son homed en el e0d).

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
-----	-----	-----	-----	-----
node1/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-
node2/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-


```
cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
```

Switch	Type	Address
Model		
-----	-----	-----
sw1	cluster-network	10.233.205.90
MSN2100-CB2RC		
Serial Number: MNXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 4.4.3 running on Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		
sw2	cluster-network	10.233.205.91
MSN2100-CB2RC		
Serial Number: MNCXXXXXXGS		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 4.4.3 running on Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		

El futuro

"Instale el archivo CSHM".

Instale el archivo de configuración del monitor de estado del switch Ethernet

Siga este procedimiento para instalar el archivo de configuración correspondiente para la supervisión del estado del switch Ethernet de los switches de clúster NVIDIA. Los modelos admitidos son:

- MSN2100-CB2FC
- MSN2100-CB2RC
- X190006-PE
- X190006-PI



Este procedimiento de instalación se aplica a ONTAP 9.10.1 y versiones posteriores.

Antes de empezar

- Verifique que necesita descargar el archivo de configuración ejecutando `system switch ethernet show` y comprobando si se muestra **OTHER** para su modelo.

Si su modelo sigue mostrando **OTHER** después de aplicar el archivo de configuración, póngase en contacto con el servicio de asistencia técnica de NetApp.

- Asegúrese de que el clúster de ONTAP esté en funcionamiento.
- Active SSH para utilizar todas las funciones disponibles en CSHM.
- Borre el `/mroot/etc/cshm_nod/nod_sign/` directorio en todos los nodos:

- a. Entra en el infierno:

```
system node run -node <name>
```

- b. Cambiar a privilegio avanzado:

```
priv set advanced
```

- c. Enumere los archivos de configuración en el `/etc/cshm_nod/nod_sign` directorio. Si el directorio existe y contiene archivos de configuración, enumera los nombres de archivo.

```
ls /etc/cshm_nod/nod_sign
```

- d. Elimine todos los archivos de configuración correspondientes a los modelos de switch conectados.

Si no está seguro, elimine todos los archivos de configuración de los modelos compatibles enumerados anteriormente y, a continuación, descargue e instale los archivos de configuración más recientes para esos mismos modelos.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

- a. Confirme que los archivos de configuración eliminados ya no están en el directorio:

```
ls /etc/cshm_nod/nod_sign
```

Pasos

1. Descargue el archivo zip de configuración del monitor de estado del switch Ethernet según la versión de ONTAP correspondiente. Este archivo está disponible en la "[Switches Ethernet de NVIDIA](#)" página.
 - a. En la página de descarga del software NVIDIA SN2100, seleccione **Nvidia CSHM File**.
 - b. En la página Precaución/debe leer, seleccione la casilla de verificación para aceptar.
 - c. En la página Contrato de licencia de usuario final, seleccione la casilla de verificación para aceptar y haga clic en **Aceptar y continuar**.
 - d. En la página Nvidia CSHM File - Download, seleccione el archivo de configuración aplicable. Están disponibles los siguientes archivos:

ONTAP 9.15.1 y versiones posteriores

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 a 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. Cargue el archivo zip correspondiente al servidor web interno.
2. Acceda a la configuración de modo avanzado desde uno de los sistemas ONTAP en el clúster.

```
set -privilege advanced
```

3. Ejecute el comando switch health monitor configure.

```
cluster1::> system cluster-switch configure-health-monitor -node *  
-package-url http://192.168.2.20/usr/download/[filename.zip]
```

4. Compruebe que el resultado del comando termine con el siguiente texto para su versión de ONTAP:

ONTAP 9.15.1 y versiones posteriores

La supervisión de estado del switch Ethernet ha instalado el archivo de configuración.

ONTAP 9.11.1 a 9.14.1

SHM instaló el archivo de configuración.

ONTAP 9.10.1

El paquete descargado de CSHM se ha procesado correctamente.

Si se produce un error, póngase en contacto con el soporte de NetApp.

1. Espere hasta dos veces el intervalo de sondeo del monitor de estado del switch Ethernet, que se encuentra ejecutando `system switch ethernet polling-interval show`, antes de completar el siguiente paso.
2. Ejecute el comando `system switch ethernet show` en el sistema ONTAP y asegúrese de que los conmutadores del clúster se descubran con el campo Monitorizado establecido en **Verdadero** y el campo de número de serie no muestre **Desconocido**.

```
cluster1::> system switch ethernet show
```

El futuro

["Configure la supervisión de estado del switch"](#).

Restablecer el interruptor de almacenamiento SN2100 a los valores predeterminados de fábrica

Para restablecer el interruptor de almacenamiento SN2100 a los valores predeterminados de fábrica:

- Para Cumulus Linux 5.10 y versiones anteriores, aplique la imagen de Cumulus.
- Para Cumulus Linux 5.11 y posteriores, utilice el `nv action reset system factory-default` dominio.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Debe tener la contraseña root para acceder a los comandos de sudo.



Para obtener más información sobre la instalación de Cumulus Linux, consulte ["Flujo de trabajo de instalación de software para los switches NVIDIA SN2100"](#).

Ejemplo 7. Pasos

Cumulus Linux 5.10 y anteriores

1. Desde la consola Cumulus, descargue y ponga en cola la instalación del software del conmutador con el comando `onie-install -a -i` Seguido de la ruta del archivo al software del conmutador, por ejemplo:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. El instalador inicia la descarga. Escriba **y** cuando se le solicite para confirmar la instalación cuando se haya descargado y verificado la imagen.
3. Reinicie el conmutador para instalar el nuevo software.

```
sudo reboot
```

```
cumulus@sw1:mgmt:~$ sudo reboot
```



El conmutador se reinicia y accede a la instalación del software del conmutador, lo que lleva algún tiempo. Cuando se completa la instalación, el conmutador se reinicia y permanece en el log-in inmediato.

Cumulus Linux 5.11 y posteriores

1. Para restablecer el interruptor a los valores predeterminados de fábrica y eliminar toda la configuración, los archivos del sistema y los archivos de registro, ejecute:

```
nv action reset system factory-default
```

Por ejemplo:

```
cumulus@switch:~$ nv action reset system factory-default
```

```
This operation will reset the system configuration, delete the log files and reboot the switch.
```

```
Type [y] continue.
```

```
Type [n] to abort.
```

```
Do you want to continue? [y/n] y
```

Ver NVIDIA ["Restablecimiento de fábrica"](#) documentación para más detalles.

Migrar switches

Migrar desde un switch de almacenamiento de Cisco a un switch de almacenamiento NVIDIA SN2100

Puede migrar switches Cisco anteriores para un clúster de ONTAP a switches de almacenamiento NVIDIA SN2100. Este procedimiento no es disruptivo.

Revise los requisitos

Se admiten los siguientes switches de almacenamiento:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- Consulte "[Hardware Universe](#)" para obtener toda la información de los puertos compatibles y sus configuraciones.

Antes de empezar

Asegúrese de tener lo siguiente:

- El clúster existente está configurado y funciona correctamente.
- Todos los puertos de almacenamiento están en estado up para garantizar operaciones no disruptivas.
- Los switches de almacenamiento NVIDIA SN2100 están configurados y funcionan con la versión adecuada de Cumulus Linux instalado con el archivo de configuración de referencia (RCF) aplicado.
- La configuración de red de almacenamiento existente tiene lo siguiente:
 - 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 en estado activo con las LIF del clúster están en sus puertos iniciales.
 - Puertos ISL habilitados y cableado entre los switches de Cisco anteriores y entre los switches nuevos.
- Consulte "[Hardware Universe](#)" para obtener toda la información de los puertos compatibles y sus configuraciones.
- Algunos puertos están configurados en switches NVIDIA SN2100 para que se ejecuten a 100 GbE.
- Ha planificado, migrado y documentado la conectividad de 100 GbE desde los nodos a los switches de almacenamiento NVIDIA SN2100.

Migrar los switches

Acerca de los ejemplos

En este procedimiento, se utilizan los switches de almacenamiento Cisco Nexus 9336C-FX2 como comandos y salidas de ejemplo.

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los switches de almacenamiento existentes Cisco Nexus 9336C-FX2 son *S1* y *S2*.
- Los nuevos switches de almacenamiento NVIDIA SN2100 son *sw1* y *sw2*.
- 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.
- La `cluster1::*>` prompt indica el nombre del clúster.
- Los puertos de red utilizados en este procedimiento son *e5a* y *e5b*.

- Los puertos de arranque toman el formato: Swp1s0-3. Por ejemplo, cuatro puertos de arranque en swp1 son *swp1s0*, *swp1s1*, *swp1s2* y *swp1s3*.
- El interruptor S2 se sustituye primero por el interruptor sw2 y luego el interruptor S1 se sustituye por el interruptor sw1.
 - El cableado entre los nodos y S2 se desconecta de S2 y se vuelve a conectar a sw2.
 - El cableado entre los nodos y S1 se desconecta de S1 y se vuelve a conectar a sw1.

Paso 1: Preparación para la migración

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
```

donde x es la duración de la ventana de mantenimiento en horas.

2. Cambie el nivel de privilegio a avanzado, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

3. Determine el estado administrativo u operativo de cada interfaz de almacenamiento:

Cada puerto debe aparecer habilitado para Status.

Paso 2: Configure los cables y los puertos

1. Mostrar los atributos del puerto de red:

```
storage port show
```

Muestra el ejemplo

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID

node1							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

- Compruebe que los puertos de almacenamiento de cada nodo están conectados a los switches de almacenamiento existentes de la siguiente manera (desde la perspectiva de los nodos) mediante el comando:

```
network device-discovery show -protocol lldp
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			

node1	/lldp		
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/1
	e5b	S2 (7c:ad:4f:98:8e:3c)	Eth1/1
node2	/lldp		
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/2
	e5b	S2 (7c:ad:4f:98:8e:3c)	Eth1/2

- En los interruptores S1 y S2, asegúrese de que los puertos de almacenamiento y los conmutadores están conectados de la siguiente manera (desde la perspectiva de los conmutadores) mediante el comando:

```
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 Port ID	Local Intf	Holdtime	Capability
node1 e0c	Eth1/1	121	S
node2 e0c	Eth1/2	121	S
SHFGD1947000186 e0a	Eth1/10	120	S
SHFGD1947000186 e0a	Eth1/11	120	S
SHFGB2017000269 e0a	Eth1/12	120	S
SHFGB2017000269 e0a	Eth1/13	120	S

```
S2# show lldp neighbors
```

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS
Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station

(O) Other

Device-ID Port ID	Local Intf	Holdtime	Capability
node1 e5b	Eth1/1	121	S
node2 e5b	Eth1/2	121	S
SHFGD1947000186 e0b	Eth1/10	120	S
SHFGD1947000186 e0b	Eth1/11	120	S
SHFGB2017000269 e0b	Eth1/12	120	S
SHFGB2017000269 e0b	Eth1/13	120	S

4. En el switch sw2, apague los puertos conectados a los nodos y los puertos de almacenamiento de las bandejas de discos.

Muestra el ejemplo

```
cumulus@sw2:~$ net add interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

5. Mueva los puertos de almacenamiento de nodos de la controladora y de las bandejas de discos del conmutador S2 antiguo al nuevo switch sw2 utilizando el cableado adecuado que admite NVIDIA SN2100.
6. En el switch sw2, conecte los puertos conectados a los puertos de almacenamiento de los nodos y las bandejas de discos.

Muestra el ejemplo

```
cumulus@sw2:~$ net del interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

7. Compruebe que los puertos de almacenamiento de cada nodo ahora están conectados a los switches de la siguiente manera, desde la perspectiva de los nodos:

```
network device-discovery show -protocol lldp
```

Muestra el ejemplo

```
cluster1::~*> network device-discovery show -protocol lldp
```

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform

node1	/lldp			
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/1	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1	-
node2	/lldp			
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/2	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2	-

8. Verifique los atributos de puerto de red:

storage port show

Muestra el ejemplo

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
node1							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

9. En el switch sw2, compruebe que todos los puertos de almacenamiento de nodos estén activos:

net show interface

Muestra el ejemplo

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					
-----	-----	----	-----	-----	-----
.....					
...					
...					
UP	swp1	100G	9216	Trunk/L2	node1 (e5b)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e5b)
Master: bridge(UP)					
UP	swp3	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp5	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
UP	swp6	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
...					
...					

10. En el switch sw1, apague los puertos conectados a los puertos de almacenamiento de los nodos y las bandejas de discos.

Muestra el ejemplo

```
cumulus@sw1:~$ net add interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

11. Mueva los puertos de almacenamiento de nodos de la controladora y las bandejas de discos del conmutador S1 antiguo al switch sw1 nuevo, utilizando el cableado adecuado que admite NVIDIA SN2100.
12. En el switch sw1, conecte los puertos conectados a los puertos de almacenamiento de los nodos y las bandejas de discos.

Muestra el ejemplo

```
cumulus@sw1:~$ net del interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

13. Compruebe que los puertos de almacenamiento de cada nodo ahora están conectados a los switches de la siguiente manera, desde la perspectiva de los nodos:

```
network device-discovery show -protocol lldp
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1	/lldp			
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp1	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1	-
node2	/lldp			
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp2	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2	-

Paso 3: Verificar la configuración

1. Compruebe la configuración final:

```
storage port show
```

Cada puerto debe aparecer habilitado para State y habilitado para Status.

Muestra el ejemplo

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID

node1	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

2. En el switch sw2, compruebe que todos los puertos de almacenamiento de nodos estén activos:

```
net show interface
```

Muestra el ejemplo

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp1	100G	9216	Trunk/L2	node1 (e5b)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e5b)
Master: bridge(UP)					
UP	swp3	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp5	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
UP	swp6	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
...					
...					

3. Compruebe que ambos nodos tengan una conexión cada uno con cada switch:

```
net show lldp
```

Muestra el ejemplo

En el siguiente ejemplo, se muestran los resultados adecuados para ambos switches:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
...				
swp1	100G	Trunk/L2	node1	e0c
swp2	100G	Trunk/L2	node2	e0c
swp3	100G	Trunk/L2	SHFFG1826000112	e0a
swp4	100G	Trunk/L2	SHFFG1826000112	e0a
swp5	100G	Trunk/L2	SHFFG1826000102	e0a
swp6	100G	Trunk/L2	SHFFG1826000102	e0a


```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
...				
swp1	100G	Trunk/L2	node1	e5b
swp2	100G	Trunk/L2	node2	e5b
swp3	100G	Trunk/L2	SHFFG1826000112	e0b
swp4	100G	Trunk/L2	SHFFG1826000112	e0b
swp5	100G	Trunk/L2	SHFFG1826000102	e0b
swp6	100G	Trunk/L2	SHFFG1826000102	e0b

4. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

5. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

El futuro

["Configure la supervisión de estado del switch"](#).

Sustituya el conmutador de almacenamiento NVIDIA SN2100

Puede sustituir un conmutador de almacenamiento NVIDIA SN2100 defectuoso. Se trata de un procedimiento no disruptivo.

Antes de empezar

Antes de instalar el software Cumulus y los RCF en un conmutador de almacenamiento NVIDIA SN2100, asegúrese de que:

- Su sistema puede admitir los switches de almacenamiento NVIDIA SN2100.
- Ha descargado los RCF correspondientes.

La "[Hardware Universe](#)" proporciona información completa sobre los puertos admitidos y sus configuraciones.

La configuración de red existente debe tener las siguientes características:

- Complete todos los pasos de solución de problemas para confirmar que necesita reemplazar su interruptor.
- Asegúrese de que exista conectividad de administración en ambos conmutadores.



Asegúrese de que se han completado todos los pasos de solución de problemas para confirmar que es necesario sustituir el interruptor.

El conmutador NVIDIA SN2100 de repuesto debe tener las siguientes características:

- La conectividad de la red de gestión es funcional.
- Puedes acceder al interruptor de reemplazo usando la consola.
- La imagen apropiada del sistema operativo RCF y Cumulus se carga en el conmutador.
- Se ha completado la personalización inicial del conmutador.

Resumen del procedimiento

Este procedimiento sustituye al segundo conmutador de almacenamiento NVIDIA SN2100 sw2 con el nuevo conmutador NVIDIA SN2100 nsw2. Los dos nodos son 1 y 2.

Pasos a completar:

- Confirmar que el interruptor que se va a sustituir es sw2.
- Desconecte los cables del interruptor sw2.
- Vuelva a conectar los cables al conmutador nsw2.
- Verifique todas las configuraciones del dispositivo en el interruptor nsw2.

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
```

x es la duración de la ventana de mantenimiento en horas.

2. Cambie el nivel de privilegio a avanzado, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

3. Verifique el estado de salud de los puertos del nodo de almacenamiento para confirmar la conexión al conmutador de almacenamiento S1:

```
storage port show -port-type ENET
```


Muestra el ejemplo

```
cluster1::*> storage port show -port-type ENET
```

				Speed			VLAN
Node	Port	Type	Mode	(Gb/s)	State	Status	ID
-----	----	-----	-----	-----	-----	-----	----
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

4. Compruebe que el interruptor sw1 de almacenamiento esté disponible:

```
network device-discovery show -protocol lldp
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1/lldp
e0M           sw1 (00:ea:bd:68:6a:e8)   Eth1/46          -
e0b           sw2 (6c:b2:ae:5f:a5:b2)   Ethernet1/16     -
e0c           SHFFG1827000286 (d0:39:ea:1c:16:92)
                                           e0a              -
e0e           sw3 (6c:b2:ae:5f:a5:ba)   Ethernet1/18     -
e0f           SHFFG1827000286 (00:a0:98:fd:e4:a9)
                                           e0b              -
e0g           sw4 (28:ac:9e:d5:4a:9c)   Ethernet1/11     -
e0h           sw5 (6c:b2:ae:5f:a5:ca)   Ethernet1/22     -
e1a           sw6 (00:f6:63:10:be:7c)   Ethernet1/33     -
e1b           sw7 (00:f6:63:10:be:7d)   Ethernet1/34     -
e2a           sw8 (b8:ce:f6:91:3d:88)   Ethernet1/35     -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

5. Ejecute el `net show interface` comando en el switch de trabajo para confirmar que puede ver tanto los nodos como todas las bandejas:

```
net show interface
```

Muestra el ejemplo

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp1	100G	9216	Trunk/L2	node1 (e3a)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e3a)
Master: bridge(UP)					
UP	swp3	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp5	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
UP	swp6	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
...					
...					

6. Compruebe los puertos de la bandeja en el sistema de almacenamiento:

```
storage shelf port show -fields remote-device, remote-port
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-device, remote-  
port  
shelf    id  remote-port  remote-device  
-----  --  -  
3.20     0   swp3         sw1  
3.20     1   -           -  
3.20     2   swp4         sw1  
3.20     3   -           -  
3.30     0   swp5         sw1  
3.20     1   -           -  
3.30     2   swp6         sw1  
3.20     3   -           -  
cluster1::*>
```

7. Retire todos los cables conectados al interruptor de almacenamiento sw2.
8. Vuelva a conectar todos los cables al interruptor de recambio nsw2.
9. Vuelva a comprobar el estado de los puertos del nodo de almacenamiento:

```
storage port show -port-type ENET
```

Muestra el ejemplo

```
cluster1::*> storage port show -port-type ENET  
  
Node      Port Type  Mode    Speed      State   Status  VLAN  
-----  -  
node1  
          e3a  ENET   storage 100    enabled online   30  
          e3b  ENET   storage 0      enabled offline  30  
          e7a  ENET   storage 0      enabled offline  30  
          e7b  ENET   storage 100   enabled online   30  
node2  
          e3a  ENET   storage 100   enabled online   30  
          e3b  ENET   storage 0      enabled offline  30  
          e7a  ENET   storage 0      enabled offline  30  
          e7b  ENET   storage 100   enabled online   30  
cluster1::*>
```

10. Compruebe que ambos conmutadores estén disponibles:

```
net device-discovery show -protocol lldp
```

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol lldp
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1/lldp
e0M           sw1  (00:ea:bd:68:6a:e8)      Eth1/46      -
e0b           sw2  (6c:b2:ae:5f:a5:b2)      Ethernet1/16  -
e0c           SHFFG1827000286 (d0:39:ea:1c:16:92)
                                     e0a          -
e0e           sw3  (6c:b2:ae:5f:a5:ba)      Ethernet1/18  -
e0f           SHFFG1827000286 (00:a0:98:fd:e4:a9)
                                     e0b          -
e0g           sw4  (28:ac:9e:d5:4a:9c)      Ethernet1/11  -
e0h           sw5  (6c:b2:ae:5f:a5:ca)      Ethernet1/22  -
e1a           sw6  (00:f6:63:10:be:7c)      Ethernet1/33  -
e1b           sw7  (00:f6:63:10:be:7d)      Ethernet1/34  -
e2a           sw8  (b8:ce:f6:91:3d:88)      Ethernet1/35  -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

11. Compruebe los puertos de la bandeja en el sistema de almacenamiento:

```
storage shelf port show -fields remote-device, remote-port
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-device, remote-  
port  
shelf    id    remote-port    remote-device  
-----  
3.20     0     swp3           sw1  
3.20     1     swp3           nsw2  
3.20     2     swp4           sw1  
3.20     3     swp4           nsw2  
3.30     0     swp5           sw1  
3.20     1     swp5           nsw2  
3.30     2     swp6           sw1  
3.20     3     swp6           nsw2  
cluster1::*>
```

12. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

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
```

El futuro

["Configure la supervisión de estado del switch".](#)

Switches compartidos

Cisco Nexus 9336C-FX2

Manos a la obra

Flujo de trabajo de instalación y configuración para conmutadores compartidos Cisco Nexus 9336C-FX2

El switch compartido Cisco Nexus 9336C-FX2 forma parte de la plataforma Cisco Nexus 9000 y se puede instalar en un armario rack de sistema de NetApp. Los switches compartidos permiten combinar la funcionalidad de clúster y almacenamiento en una configuración de switch compartido, ya que admiten el uso de archivos de configuración de referencia de almacenamiento y clúster compartidos.

Siga estos pasos de flujo de trabajo para instalar y configurar sus conmutadores Cisco 9336C-FX2.

1

"Revisar los requisitos de configuración"

Revise los requisitos de configuración para el conmutador compartido 9336C-FX2.

2

"Revise los componentes y números de pieza"

Revise los componentes y números de pieza del conmutador compartido 9336C-FX2.

3

"Revisar la documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores 9336C-FX2 y el clúster ONTAP .

Requisitos de configuración de los switches compartidos Cisco Nexus 9336C-FX2

En lo que respecta a la instalación y el mantenimiento de los switches Cisco Nexus 9336C-FX2, asegúrese de revisar los requisitos de configuración y red.

Soporte de ONTAP

Desde ONTAP 9.9.1, puede utilizar los switches Cisco Nexus 9336C-FX2 para combinar la funcionalidad de almacenamiento y clúster en una configuración de switch compartido.

Si desea crear clústeres de ONTAP con más de dos nodos, necesita dos switches de red compatibles.

Requisitos de configuración

Para la configuración, necesita el número y tipo adecuados de cables y conectores de cable para los conmutadores.

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 AFF A700 de AFF, la interfaz e0M utiliza un puerto Ethernet dedicado.
- Consulte la ["Hardware Universe"](#) para obtener la información más reciente.

Para obtener más información acerca de la configuración inicial del switch, consulte la siguiente guía: ["Guía de instalación y actualización de Cisco Nexus 9336C-FX2"](#).

¿Qué sigue?

["Componentes y números de pieza"](#) .

Los componentes y números de pieza de los switches compartidos Cisco Nexus 9336C-FX2

En lo que respecta a la instalación y el mantenimiento del switch Cisco Nexus 9336C-FX2, asegúrese de revisar la lista de componentes y sus números de pieza.

En la tabla siguiente se enumeran el número de pieza y la descripción del switch 9336C-FX2, sus ventiladores y fuentes de alimentación:

Número de pieza	Descripción
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190002	Kit de accesorios X190001/X190003
X-NXA-PAC-1100W-PE2	Fuente de alimentación de 1100 W ac N9K-9336C: Flujo de aire de escape lateral del puerto
X-NXA-PAC-1100W-PI2	Fuente de alimentación de 1100 W ac N9K-9336C - flujo de aire de entrada lateral del puerto
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, flujo de aire del lado de la lumbreira
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, flujo de aire de entrada lateral de la lumbreira

¿Qué sigue?

["Documentación requerida"](#) .

Requisitos de documentación de los switches compartidos Cisco Nexus 9336C-FX2

En lo que respecta a la instalación y el mantenimiento de los switches Cisco Nexus 9336C-FX2, asegúrese de revisar la documentación específica de los switches y la

controladora para configurar sus switches Cisco 9336-FX2 y su clúster ONTAP.

Para configurar los switches compartidos Cisco Nexus 9336C-FX2, consulte ["Compatibilidad con los switches Cisco Nexus serie 9000"](#) página.

Título del documento	Descripción
"Guía de instalación de hardware de Nexus serie 9000"	Proporciona información detallada acerca de los requisitos del sitio, detalles del switch de hardware y las opciones de instalación.
"Guías de configuración del software del switch Cisco Nexus serie 9000" (Elija la guía de la versión NX-OS instalada en sus switches)	Proporciona la información inicial de configuración del switch que necesita para poder configurar el switch para el funcionamiento de ONTAP.
"Guía de actualización y degradación del software Cisco Nexus serie 9000 NX-OS" (Elija la guía de la versión NX-OS instalada en sus switches)	Proporciona información sobre cómo degradar el switch a software de switch compatible con ONTAP, si es necesario.
"Índice principal de referencia de comandos Cisco Nexus serie 9000 NX-OS"	Proporciona vínculos a las diferentes referencias de comandos proporcionadas por Cisco.
"Referencia de MIBs de Cisco Nexus 9000"	Describe los archivos de la base de datos de información de gestión (MIB) para los switches Nexus 9000.
"Referencia de mensajes del sistema Nexus serie 9000 NX-OS"	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.
"Notas de la versión de Cisco Nexus serie 9000 NX-OS" (Elija las notas para la versión de NX-OS instalada en sus 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.

Instale el hardware

Flujo de trabajo de instalación de hardware para conmutadores compartidos Cisco Nexus 9336C-FX2

Para instalar y configurar el hardware de un conmutador compartido 9336C-FX2, siga estos pasos:

1

["Complete la hoja de trabajo 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.

2

"Instale el interruptor"

Instale el interruptor 9336C-FX2.

3

"Instale el interruptor en un armario NetApp"

Instale el conmutador 9336C-FX2 y el panel de paso en un gabinete NetApp según sea necesario.

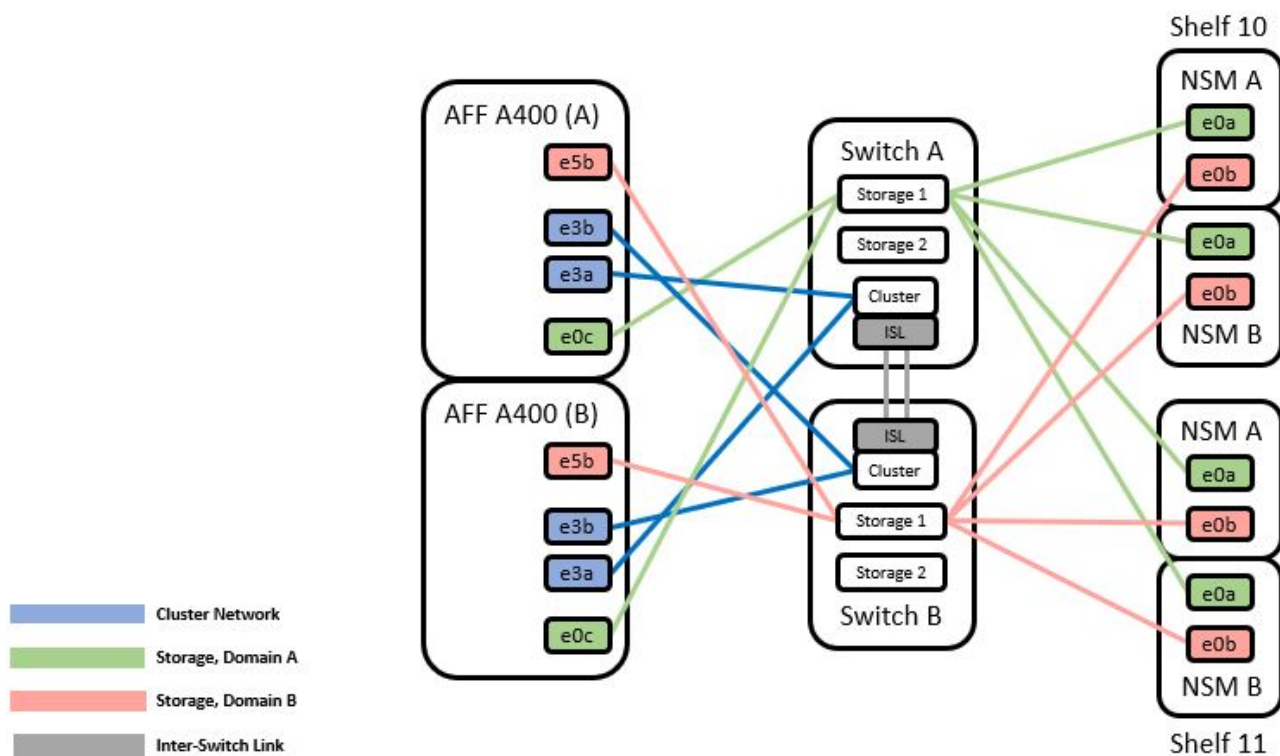
Rellene la hoja de trabajo del cableado Cisco Nexus 9336C-FX2

Utilice las siguientes imágenes de cableado para completar el cableado entre las controladoras y los switches.

Almacenamiento de cable NS224 como conectado a conmutador

Si desea conectar el cable de almacenamiento NS224 como conmutador, siga el diagrama conectado al conmutador:

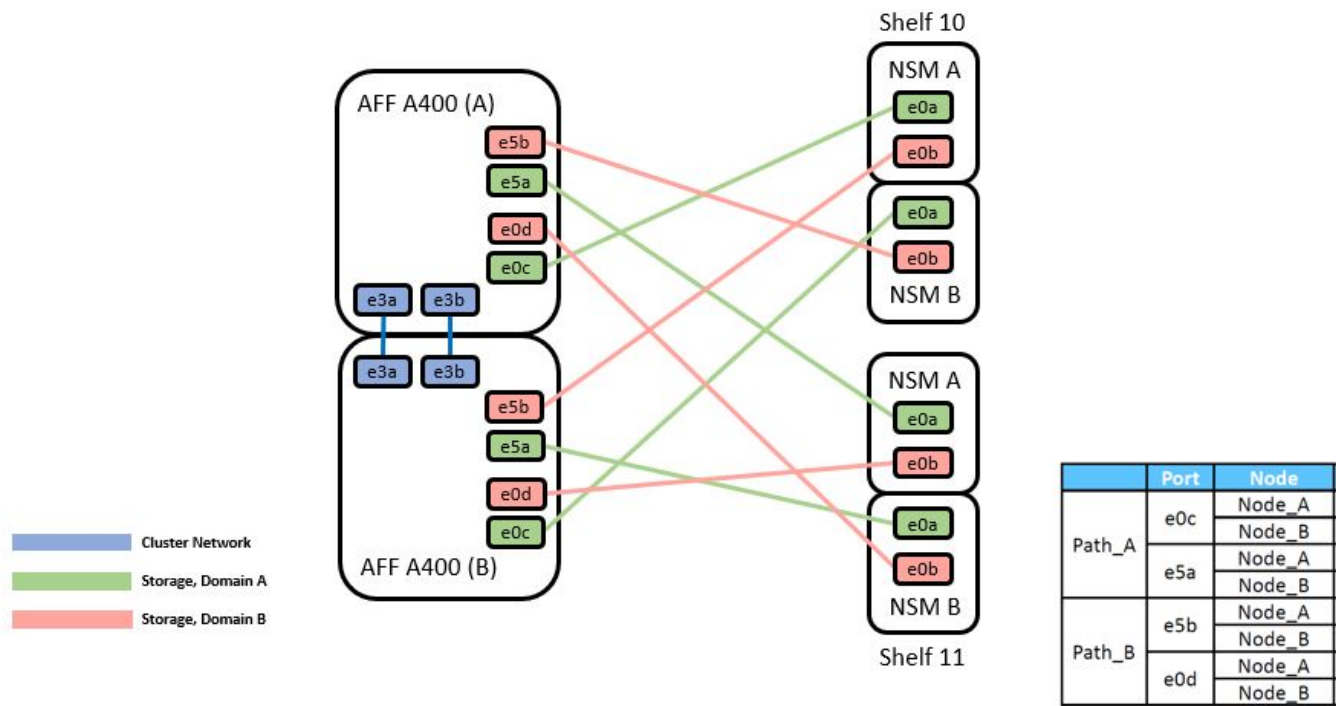
Switch Attached



Consulte "[Hardware Universe](#)" para obtener más información sobre los puertos de switch.

Almacenamiento de cable NS224 como conexión directa

Si desea conectar mediante cable el almacenamiento NS224 como de conexión directa en lugar de utilizar los puertos de almacenamiento del conmutador compartido, siga el diagrama de conexión directa:



Consulte "[Hardware Universe](#)" para obtener más información sobre los puertos de switch.

Hoja de trabajo del cableado Cisco Nexus 9336C-FX2

Si desea documentar las plataformas compatibles, debe rellenar la hoja de datos de cableado en blanco utilizando la hoja de datos de cableado de muestra completada como guía.

La definición de puerto de ejemplo de cada par de conmutadores es la siguiente:

Switch A			Switch B		
Switch Port	Port Role	Port Usage	Switch Port	Port Role	Port Usage
1	Cluster	40/100GbE	1	Cluster	40/100GbE
2	Cluster	40/100GbE	2	Cluster	40/100GbE
3	Cluster	40/100GbE	3	Cluster	40/100GbE
4	Cluster	40/100GbE	4	Cluster	40/100GbE
5	Cluster	40/100GbE	5	Cluster	40/100GbE
6	Cluster	40/100GbE	6	Cluster	40/100GbE
7	Cluster	40/100GbE	7	Cluster	40/100GbE
8	Cluster	40/100GbE	8	Cluster	40/100GbE
9	Cluster	40GbE w/4x10GbE b/o	9	Cluster	40GbE w/4x10GbE b/o
10	Cluster	100GbE w/4x25GbE b/o	10	Cluster	100GbE w/4x25GbE b/o
11	Storage	100GbE	11	Storage	100GbE
12	Storage	100GbE	12	Storage	100GbE
13	Storage	100GbE	13	Storage	100GbE
14	Storage	100GbE	14	Storage	100GbE
15	Storage	100GbE	15	Storage	100GbE
16	Storage	100GbE	16	Storage	100GbE
17	Storage	100GbE	17	Storage	100GbE
18	Storage	100GbE	18	Storage	100GbE
19	Storage	100GbE	19	Storage	100GbE
20	Storage	100GbE	20	Storage	100GbE
21	Storage	100GbE	21	Storage	100GbE
22	Storage	100GbE	22	Storage	100GbE
23	Storage	100GbE	23	Storage	100GbE
24	Storage	100GbE	24	Storage	100GbE
25	Storage	100GbE	25	Storage	100GbE
26	Storage	100GbE	26	Storage	100GbE
27	Storage	100GbE	27	Storage	100GbE
28	Storage	100GbE	28	Storage	100GbE
29	Storage	100GbE	29	Storage	100GbE
30	Storage	100GbE	30	Storage	100GbE
31	Storage	100GbE	31	Storage	100GbE
32	Storage	100GbE	32	Storage	100GbE
33	Storage	100GbE	33	Storage	100GbE
34	Storage	100GbE	34	Storage	100GbE
35	ISL	100GbE	35	ISL	100GbE
36	ISL	100GbE	36	ISL	100GbE

Donde:

- ISL DE 100 G para cambiar al puerto 35
- ISL DE 100 G para cambiar al puerto 36
- 100G ISL al puerto 35 del switch B.
- 100G ISL al puerto 36 del switch B.

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 tabla conexiones de clúster admitidas del Hardware Universe define los puertos de clúster que utiliza la plataforma.

Switch Port	Switch A Port Role	Port Usage	Switch Port	Switch B Port Role	Port Usage
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		
20			20		
21			21		
22			22		
23			23		
24			24		
25			25		
26			26		
27			27		
28			28		
29			29		
30			30		
31			31		
32			32		
33			33		
34			34		
35			35		
36			36		

Donde:

- ISL DE 100 G para cambiar al puerto 35
- ISL DE 100 G para cambiar al puerto 36
- 100G ISL al puerto 35 del switch B.
- 100G ISL al puerto 36 del switch B.

¿Qué sigue?

"Instale el interruptor".

Instale los switches compartidos Cisco Nexus 9336C-FX2

Siga estas instrucciones para configurar los switches compartidos Cisco Nexus 9336C-FX2.

Antes de empezar

Asegúrese de tener lo siguiente:

- Se requiere documentación de los switches compartidos, documentación de la controladora y documentación de ONTAP. Consulte ["Requisitos de documentación de los switches compartidos Cisco Nexus 9336C-FX2"](#) y.. ["Documentación de ONTAP de NetApp"](#).
- Las licencias aplicables, la información de configuración y red, y los cables.
- Hojas de datos de cableado completadas. Consulte ["Rellene la hoja de trabajo del cableado Cisco Nexus 9336C-FX2"](#). Para obtener más información sobre el cableado, consulte ["Hardware Universe"](#).

Pasos

1. Monte en rack los switches, las controladoras y las bandejas de almacenamiento NVMe NS224.

Consulte el ["Instrucciones de la estantería"](#) para obtener información sobre cómo montar en rack el switch en un armario NetApp.

2. Encienda los switches, las controladoras y las bandejas de almacenamiento NVMe NS224.

El futuro

Opcionalmente, puedes ["Instale un switch Cisco Nexus 9336C-FX2 en un armario de NetApp"](#). De lo contrario, vaya a ["Configure el switch"](#).

Instale un switch Cisco Nexus 9336C-FX2 en un armario de NetApp

En función de la configuración existente, es posible que tenga que instalar el switch Cisco Nexus 9336C-FX2 y el panel de paso a través en un armario de NetApp. Con el interruptor se incluyen soportes estándar.

Antes de empezar

Asegúrese de tener lo siguiente:

- Para cada interruptor, debe suministrar los ocho tornillos 10-32 ó 12-24 y tuercas de abrazadera para montar los soportes y rieles deslizantes en los postes del armario delantero y trasero.
- Debe utilizar el kit de raíl estándar de Cisco para instalar el switch en un armario 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).

Documentación requerida

Revise los requisitos iniciales de preparación, el contenido del kit y las precauciones de seguridad en la ["Guía de instalación de hardware de Cisco Nexus serie 9000"](#).

Pasos

1. Instale el panel de borrado de paso en el armario de NetApp.

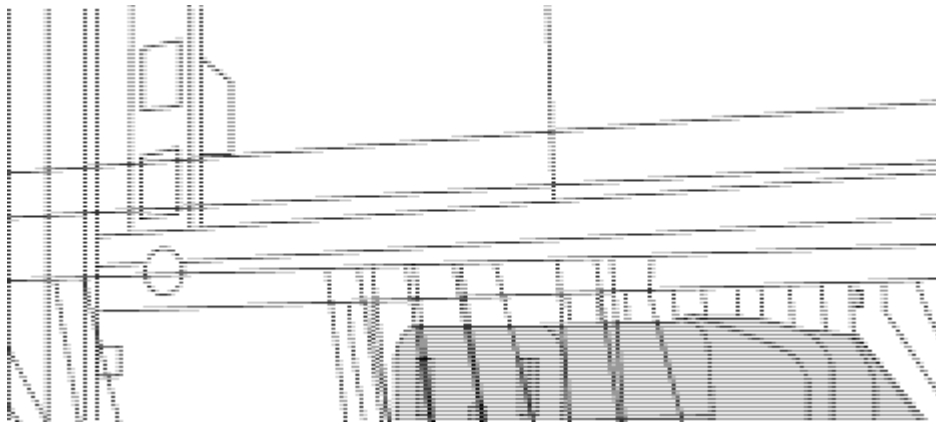
NetApp puede adquirir el kit de panel de paso a través (número de pieza X8784-R6).

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.

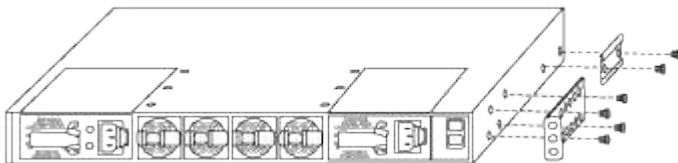
- ii. Instale dos tuercas de abrazadera a cada lado en los orificios cuadrados adecuados para los rieles delanteros del armario.
- iii. Centre el panel verticalmente para evitar intrusiones en el espacio adyacente del bastidor y, a continuación, apriete los tornillos.
- iv. Inserte los conectores hembra 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.

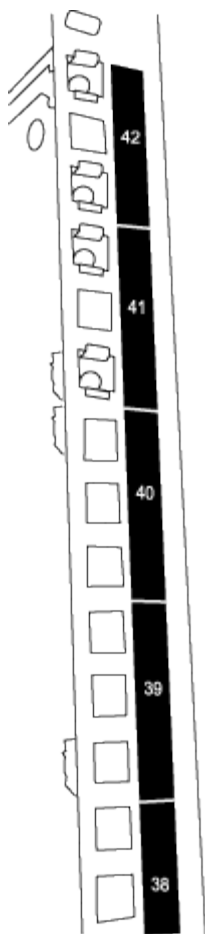
2. Instale los soportes de montaje en rack en el chasis del switch Nexus 9336C-FX2.

- 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.

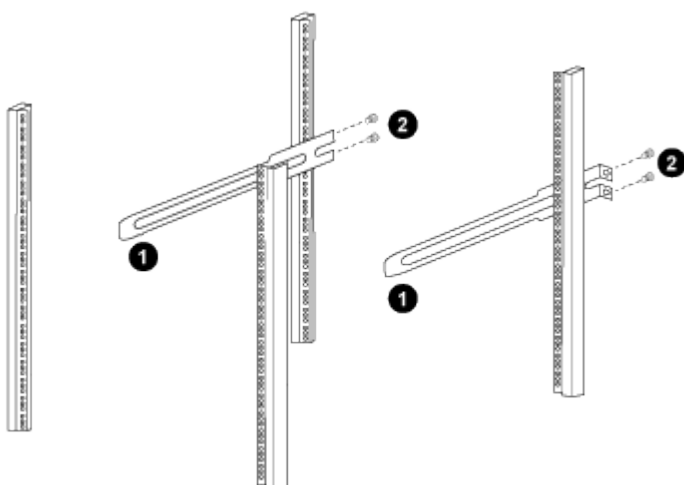
3. Instale las tuercas de abrazadera en las ubicaciones de los orificios cuadrados de los cuatro postes de IEA.



Los dos conmutadores 9336C-FX2 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.

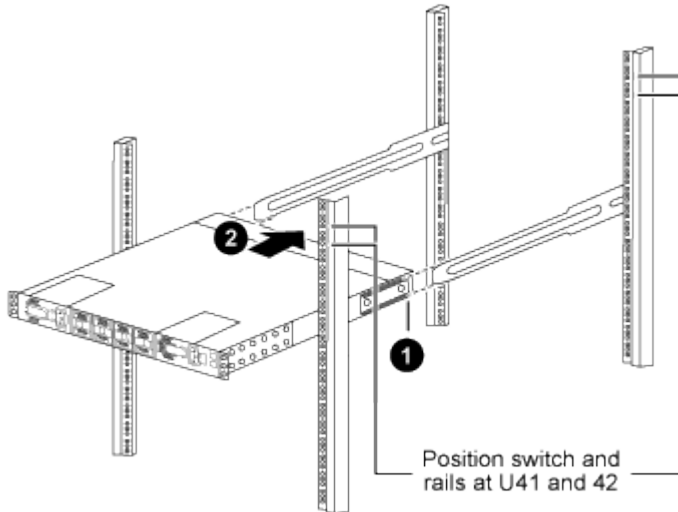
(2) apriete los tornillos de las guías deslizantes a los postes del armario.

- 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.

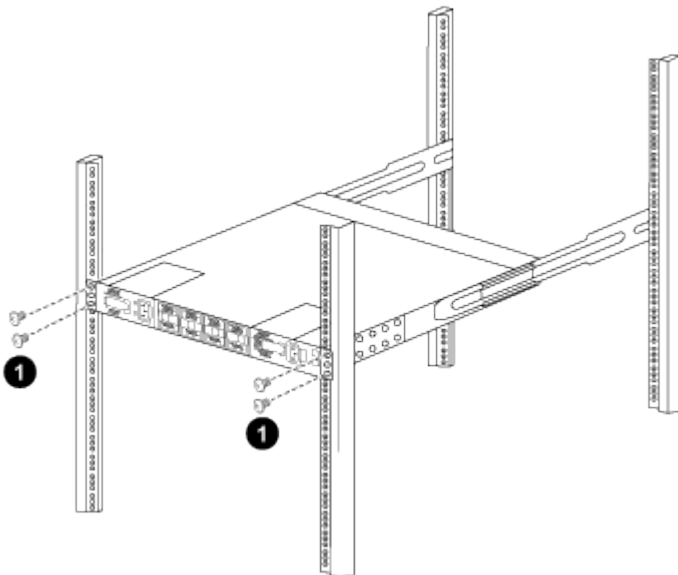
- a. Coloque la parte posterior del interruptor en RU41.



(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 delantera 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 9336C-FX2 a cualquiera de los switches de administración (si se 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.

Configurar el software

Flujo de trabajo de instalación de software para switches compartidos Cisco Nexus 9336C-FX2

Para instalar y configurar software para un switch compartido Cisco Nexus 9336C-FX2, siga estos pasos:

1

"Configure el switch"

Configurar el conmutador compartido 9336C-FX2.

2

"Prepárese para instalar el software NX-OS y RCF"

El software Cisco NX-OS y los archivos de configuración de referencia (RCF) deben estar instalados en los conmutadores compartidos Cisco 9336C-FX2.

3

"Instale o actualice el software NX-OS"

Descargue e instale o actualice el software NX-OS en el conmutador compartido Cisco 9336C-FX2.

4

"Instale el RCF"

Instale el RCF después de configurar el conmutador compartido Cisco 9336C-FX2 por primera vez.

5

"Actualice su RCF"

Actualice su versión RCF cuando tenga una versión existente del archivo RCF instalada en sus conmutadores operativos.

"Restablecer el interruptor a los valores predeterminados de fábrica"

Borre la configuración del conmutador compartido 9336C-FX2.

Configurar los switches compartidos Cisco Nexus 9336C-FX2

Siga estas instrucciones para configurar los switches compartidos Cisco Nexus 9336C-FX2.

Antes de empezar

Asegúrese de tener lo siguiente:

- Se requiere documentación de los switches compartidos, documentación de la controladora y documentación de ONTAP. Consulte ["Requisitos de documentación de los switches compartidos Cisco Nexus 9336C-FX2"](#) y.. ["Documentación de ONTAP de NetApp"](#).
- Las licencias aplicables, la información de configuración y red, y los cables.
- Hojas de datos de cableado completadas. Consulte ["Rellene la hoja de trabajo del cableado Cisco Nexus 9336C-FX2"](#). Para obtener más información sobre el cableado, consulte ["Hardware Universe"](#).

Pasos

1. realice una configuración inicial de los interruptores.

Para la configuración, necesita el número y tipo adecuados de cables y conectores de cable para los conmutadores.

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.

2. Arranque el interruptor.

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.

- a. ¿Desea anular el aprovisionamiento automático y continuar con la configuración normal? (sí/no)

Responda con **sí**. El valor predeterminado es no

- b. ¿Desea aplicar un estándar de contraseña segura? (sí/no)

Responda con **sí**. El valor predeterminado es yes.

- c. Introduzca la contraseña para el administrador.

La contraseña predeterminada es admin, pero debe crear una contraseña nueva.

Se puede rechazar una contraseña débil.

- d. ¿Desea introducir el cuadro de diálogo de configuración básica? (sí/no)

Responda con **sí** en la configuración inicial del interruptor.

e. ¿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

f. ¿Configurar cadena de comunidad SNMP de solo lectura? (sí/no)

Responda con **no**. El valor predeterminado es no

g. ¿Configurar cadena de comunidad SNMP de lectura y escritura? (sí/no)

Responda con **no**. El valor predeterminado es no

h. Introduzca el nombre del switch.

El nombre del conmutador está limitado a 63 caracteres alfanuméricos.

i. ¿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

j. ¿Configurar la puerta de enlace predeterminada? (sí/no)

Responda con **sí**. En la dirección IPv4 de la solicitud default-Gateway:, introduzca su default_Gateway.

k. ¿Configurar las opciones avanzadas de IP? (sí/no)

Responda con **no**. El valor predeterminado es no

l. ¿Habilitar el servicio telnet? (sí/no)

Responda con **no**. El valor predeterminado es no

m. ¿Habilitar el servicio SSH? (sí/no)

Responda con **sí**. El valor predeterminado es yes.



Se recomienda SSH cuando se utiliza Ethernet Switch Health Monitor (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.

a. Introduzca el tipo de clave SSH que desea generar (dsa/rsa/rsa1). El valor predeterminado es rsa.

b. Introduzca el número de bits de clave (1024- 2048).

c. ¿Configurar el servidor NTP? (sí/no)

Responda con **no**. El valor predeterminado es no

d. Configurar la capa de interfaz predeterminada (L3/L2):

Responda con **L2**. El valor predeterminado es L2.

e. Configurar el estado predeterminado de la interfaz del puerto del switch (cerrada/nohut):

Responda con **nohut**. El valor predeterminado es nohut.

f. Configurar el perfil del sistema COPP (estricto/moderado/indulgente/denso):

Responda con **estricto**. El valor predeterminado es estricto.

g. ¿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 sin que aparezca el mensaje. Responda con **sí** si desea editar los ajustes de configuración.

h. ¿Utilizar esta configuración y guardarla? (sí/no)

Responda con **sí** para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.

3. Compruebe las opciones de configuración que ha realizado en la pantalla que aparece al final de la instalación y asegúrese de guardar la configuración.



Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador.

4. 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"](#).

Prepárese para instalar el software NX-OS y RCF

Antes de instalar el software NX-OS y el archivo de configuración de referencia (RCF), siga este procedimiento.

Documentación sugerida

- ["Página del switch Cisco Ethernet"](#)

Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.

- ["Guías de actualización y degradación de software"](#)

Consulte las guías de software y actualización correspondientes disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación del conmutador Cisco.

- ["Matriz de ISSU y actualización de Cisco Nexus 9000 y 3000"](#)

Proporciona información sobre actualizaciones o desactualizaciones disruptivas para el software Cisco NX-OS en los conmutadores Nexus serie 9000 en función de sus versiones actuales y futuras.

En la página, selecciona **Actualización disruptiva** y selecciona tu versión actual y la versión de destino de la lista desplegable.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de nodo son cluster1-01 y cluster1-02.
- Los nombres de las LIF de 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 9000; 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	N9K-
C9336C	e0b	cs2	Eth1/2	N9K-
C9336C				
cluster1-01/cdp	e0a	cs1	Eth1/1	N9K-
C9336C	e0b	cs2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

4. Compruebe el estado administrativo u operativo de cada interfaz 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						

```
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
```

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					

node1					
	3/5/2022 19:21:18 -06:00		cluster1-01_clus2		cluster1-02-
clus1	none				
	3/5/2022 19:21:20 -06:00		cluster1-01_clus2		cluster1-
02_clus2	none				
node2					
	3/5/2022 19:21:18 -06:00		cluster1-02_clus2		cluster1-
01_clus1	none				
	3/5/2022 19:21:20 -06:00		cluster1-02_clus2		cluster1-
01_clus2	none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01 e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. Verifique que el comando de reversión automática esté habilitado en todas las LIF 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.

El futuro

["Instale el software NX-OS".](#)

Instale el software NX-OS

Siga este procedimiento para instalar el software NX-OS en el switch compartido Nexus 9336C-FX2.

Antes de comenzar, complete el procedimiento en ["Prepare la instalación de NX-OS y RCF".](#)

Revise los requisitos

Antes de empezar

Asegúrese de tener lo siguiente:

- 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

- ["Página del switch Cisco Ethernet"](#)

Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.

- ["Guías de actualización y degradación de software"](#)

Consulte las guías de software y actualización correspondientes disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación del conmutador Cisco.

- ["Matriz de ISSU y actualización de Cisco Nexus 9000 y 3000"](#)

Proporciona información sobre actualización/degradación disruptiva para software Cisco NX-OS en los switches de la serie Nexus 9000

en función de tus versiones actuales y objetivo.

En la página, selecciona **Actualización disruptiva** y selecciona tu versión actual y la versión de destino de la lista desplegable.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches de Cisco son cs1 y cs2.
- Los nombres de nodo son cluster1-01, cluster1-02, cluster1-03 y cluster1-04.
- Los nombres de las 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.

Instale el software

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.

Pasos

1. Conecte el switch de clúster a la red de gestión.
2. Utilice el comando ping 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 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. 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      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C-FX2
cluster1::*>
```

4. Compruebe el estado administrativo y operativo de cada puerto del clúster.

a. Compruebe que todos los puertos del clúster están **up** con un 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
```

	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			
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                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.90      N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                     cluster-network     10.233.205.91      N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

6. Copie las imágenes del software NX-OS y EPLD en el switch Nexus 9336C-FX2.

Muestra el ejemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.5.img /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. 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 08.38
  NXOS: version 9.3(4)
  BIOS compile time: 05/29/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]

Hardware
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash: 53298520 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

8. Instale la imagen NX-OS.

La instalación del archivo de imagen hace que se cargue cada vez que se reinicia el conmutador.

Muestra el ejemplo

```
cs2# install all nxos bootflash:nxos.9.3.5.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

```
Verifying image type.  
[] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.  
[] 100% -- SUCCESS
```

```
Performing module support checks.  
[] 100% -- SUCCESS
```

```
Notifying services about system upgrade.  
[] 100% -- SUCCESS
```

Compatibility check is done:

Module	Bootable	Impact	Install-type	Reason
1	yes	Disruptive	Reset	Default upgrade is not hitless

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt)	New-
Version		Upg-Required	
1	nxos	9.3(4)	9.3(5)
yes			
1	bios	v08.37(01/28/2020):v08.23(09/23/2015)	
v08.38(05/29/2020)		yes	

```
Switch will be reloaded for disruptive upgrade.
```

```
Do you want to continue with the installation (y/n)? [n] y
```

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[ ] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[ ] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[ ] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[ ] 100% -- SUCCESS
```

```
Finishing the upgrade, switch will reboot in 10 seconds.
```

9. 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 05.33
  NXOS: version 9.3(5)
  BIOS compile time: 09/08/2018
  NXOS image file is: bootflash:///nxos.9.3.5.bin
  NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

```
  cisco Nexus9000 C9336C-FX2 Chassis
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: cs2
  bootflash: 53298520 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```



```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
```

```
Reason: Reset due to upgrade
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

10. Actualice la imagen 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.9.3.5.img module all
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

11. Tras reiniciar el 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

12. 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 -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.

```
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	

cluster1-01/cdp	e0a	cs1	Ethernet1/7	N9K-
C9336C-FX2	e0d	cs2	Ethernet1/7	N9K-
C9336C-FX2				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C-FX2	e0d	cs2	Ethernet1/8	N9K-
C9336C-FX2				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/1	N9K-
C9336C-FX2				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N9K-
C9336C-FX2	e0b	cs2	Ethernet1/1/2	N9K-
C9336C-FX2				

```
cluster1::*> system cluster-switch show -is-monitoring-enabled  
-operational true
```

Switch Model	Type	Address	

cs1	cluster-network	10.233.205.90	N9K-
C9336C-FX2			
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	N9K-

```

C9336C-FX2
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

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.

```

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 6 a 13 para instalar el software NX-OS en el interruptor CS1.

15. Habilite la reversión automática en las LIF del clúster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```


16. 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 LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

El futuro

"[Instale el RCF](#)".

Instalación del archivo de configuración de referencia (RCF)

Puede instalar el archivo de configuración de referencia (RCF) después de configurar el conmutador Nexus 9336C-FX2 por primera vez.

Antes de comenzar, complete el procedimiento en "[Prepare la instalación de NX-OS y RCF](#)".

Antes de empezar

Compruebe las siguientes instalaciones y conexiones:

- Una conexión de consola al interruptor. La conexión de la consola es opcional si tiene acceso remoto al conmutador.
- El switch CS1 y el switch CS2 se encienden y la configuración inicial del switch se ha completado (la dirección IP de gestión y SSH está configurada).
- Se ha instalado la versión deseada de NX-OS.
- Se conectan las conexiones de enlace entre switches (ISL) entre los switches.
- Los puertos del clúster de nodos de ONTAP no están conectados.

Paso 1: Instale el RCF en los interruptores

1. Inicie sesión en el switch CS1 mediante SSH o mediante una consola de serie.
2. Copie el RCF al bootflash del switch CS1 usando 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 9000"](#).

Muestra el ejemplo

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

3. Aplique el RCF descargado 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 9000"](#).

Muestra el ejemplo

En este ejemplo se muestra el archivo RCF Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt se está instalando en el interruptor cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

4. Examine el resultado del banner desde el `show banner motd` comando. Debe leer y seguir estas instrucciones para asegurarse de que la configuración y el funcionamiento del interruptor son correctos.

Muestra el ejemplo

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Nexus N9K-C9336C-FX2
* Filename  : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date      : 10-23-2020
* Version   : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

5. 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.

6. Registre cualquier adición personalizada entre la actual `running-config` archivo y el archivo RCF en uso.
7. Después de verificar que las versiones de RCF y las configuraciones de los conmutadores sean correctas, copie el archivo `running-config` archivo al `startup-config` archivo.

```
cs1# copy running-config startup-config
[#####] 100% Copy complete
```

8. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) Para más detalles.

10. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

```
show file bootflash:write_erase.cfg
```

11. Ejecute el comando `WRITE BORRATE` para borrar la configuración guardada actual:

```
cs1# write erase
```

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] **y**

12. Copie la configuración básica guardada anteriormente en la configuración de inicio.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

13. Reinicie el interruptor CS1.

```
cs1# reload
```

This command will reboot the system. (y/n)? [n] **y**

14. Repita los pasos 1 al 13 en el interruptor cs2.

15. Conecte los puertos de clúster de todos los nodos del clúster de ONTAP a los switches CS1 y CS2.

Paso 2: Verifique las conexiones del interruptor

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
show interface brief
```

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 los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/35, Eth1/36, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
17	VLAN0017	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
18	VLAN0018	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6, Eth1/7, Eth1/8, Eth1/9/1, Eth1/9/2, Eth1/9/3, Eth1/9/4, Eth1/10/1, Eth1/10/2, Eth1/10/3, Eth1/10/4
31	VLAN0031	active	Eth1/11, Eth1/12, Eth1/13, Eth1/14, Eth1/15, Eth1/16, Eth1/17, Eth1/18, Eth1/19, Eth1/20, Eth1/21, Eth1/22
32	VLAN0032	active	Eth1/23, Eth1/24, Eth1/25

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
Eth1/34

```

```
cs1# show interface trunk
```

```

-----
Port                Native  Status      Port
                   Vlan                                Channel
-----
Eth1/1              1      trunking    --
Eth1/2              1      trunking    --
Eth1/3              1      trunking    --
Eth1/4              1      trunking    --
Eth1/5              1      trunking    --
Eth1/6              1      trunking    --
Eth1/7              1      trunking    --
Eth1/8              1      trunking    --
Eth1/9/1            1      trunking    --
Eth1/9/2            1      trunking    --
Eth1/9/3            1      trunking    --
Eth1/9/4            1      trunking    --
Eth1/10/1           1      trunking    --
Eth1/10/2           1      trunking    --
Eth1/10/3           1      trunking    --
Eth1/10/4           1      trunking    --
Eth1/11             33     trunking    --

```

Eth1/12	33	trunking	--
Eth1/13	33	trunking	--
Eth1/14	33	trunking	--
Eth1/15	33	trunking	--
Eth1/16	33	trunking	--
Eth1/17	33	trunking	--
Eth1/18	33	trunking	--
Eth1/19	33	trunking	--
Eth1/20	33	trunking	--
Eth1/21	33	trunking	--
Eth1/22	33	trunking	--
Eth1/23	34	trunking	--
Eth1/24	34	trunking	--
Eth1/25	34	trunking	--
Eth1/26	34	trunking	--
Eth1/27	34	trunking	--
Eth1/28	34	trunking	--
Eth1/29	34	trunking	--
Eth1/30	34	trunking	--
Eth1/31	34	trunking	--
Eth1/32	34	trunking	--
Eth1/33	34	trunking	--
Eth1/34	34	trunking	--
Eth1/35	1	trnk-bndl	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	1	trunking	--

```

-----
Port          Vlans Allowed on Trunk
-----
Eth1/1        1,17-18
Eth1/2        1,17-18
Eth1/3        1,17-18
Eth1/4        1,17-18
Eth1/5        1,17-18
Eth1/6        1,17-18
Eth1/7        1,17-18
Eth1/8        1,17-18
Eth1/9/1      1,17-18
Eth1/9/2      1,17-18
Eth1/9/3      1,17-18
Eth1/9/4      1,17-18
Eth1/10/1     1,17-18
Eth1/10/2     1,17-18
Eth1/10/3     1,17-18
Eth1/10/4     1,17-18

```



```

Eth1/11      31,33
Eth1/12      31,33
Eth1/13      31,33
Eth1/14      31,33
Eth1/15      31,33
Eth1/16      31,33
Eth1/17      31,33
Eth1/18      31,33
Eth1/19      31,33
Eth1/20      31,33
Eth1/21      31,33
Eth1/22      31,33
Eth1/23      32,34
Eth1/24      32,34
Eth1/25      32,34
Eth1/26      32,34
Eth1/27      32,34
Eth1/28      32,34
Eth1/29      32,34
Eth1/30      32,34
Eth1/31      32,34
Eth1/32      32,34
Eth1/33      32,34
Eth1/34      32,34
Eth1/35      1
Eth1/36      1
Po1          1
..
..
..
..
..

```



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

3. 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      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

Paso 3: Configure el cluster ONTAP

NetApp recomienda usar System Manager para configurar clústeres nuevos.

System Manager proporciona un flujo de trabajo sencillo y sencillo para la instalación y la configuración del clúster, incluidas la asignación de una dirección IP de gestión de nodos, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento del almacenamiento inicial.

Vaya a ["Configure ONTAP en un nuevo clúster con System Manager"](#) para obtener instrucciones de configuración.

El futuro

["Configure la supervisión de estado del switch"](#).

Actualice su archivo de configuración de referencia (RCF)

Actualice la versión de RCF cuando tenga instalada una versión existente del archivo RCF en los conmutadores operativos.

Antes de empezar

Asegúrese de tener lo siguiente:

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El RCF actual.
- Si está actualizando la versión de RCF, necesita una configuración de inicio en el RCF que refleje las imágenes de inicio deseadas.

Si necesita cambiar la configuración 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.



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.



Antes de instalar una nueva versión de software del conmutador y RCF, debe borrar los ajustes del conmutador y realizar la configuración básica. Debe estar conectado al switch mediante la consola serie o haber conservado la información básica de configuración antes de borrar la configuración del switch.

Paso 1: Prepárese para la actualización

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      N9K-
C9336C
          e0d    cs2                Ethernet1/7      N9K-
C9336C
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C
          e0d    cs2                Ethernet1/8      N9K-
C9336C
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C
cluster1::*>
```

2. Compruebe el estado administrativo y operativo de cada puerto del clúster.

a. Compruebe que todos los puertos del clúster están **up** con un 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
```

	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			
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                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.90      N9K-
C9336C
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                     cluster-network     10.233.205.91      N9K-
C9336C
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

3. Deshabilite la reversión automática en las LIF del clúster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
false
```

Paso 2: Configurar puertos

1. En el switch de clúster cs1, apague los puertos conectados a los puertos del clúster de los nodos.

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
```

```
cs1(config-if-range)# shutdown
```



Asegúrese de cerrar * todos * puertos de clúster conectados para evitar cualquier problema de conexión de red. Consulte el artículo de la base de conocimientos ["Nodo fuera de quórum al migrar LIF de clúster durante la actualización del sistema operativo del switch"](#) para obtener más información.

2. Compruebe que las LIF del clúster han conmutado al nodo de respaldo a los puertos alojados en el switch del clúster CS1. 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::*>				

3. 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::*>
```

4. 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
```

- Registre cualquier adición personalizada entre la configuración actual y el archivo RCF en uso (como una configuración SNMP para su organización).
 - Para NX-OS 10,2 y posterior, utilice el `show diff running-config` comando para comparar con el archivo RCF guardado en el bootflash. De lo contrario, utilice una herramienta de comparación o de diferencia de terceros.
5. Guarde los detalles básicos de la configuración en el archivo `write_erase.cfg` en el bootflash.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg
```

```
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

```
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

6. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg
```

```
cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) Para más detalles.

7. Verifique que el archivo `write_erase.cfg` se complete como se esperaba:

```
show file bootflash:write_erase.cfg
```

8. Ejecute el comando WRITE BORRATE para borrar la configuración guardada actual:

```
cs1# write erase
```

```
Warning: This command will erase the startup-configuration.
```

```
Do you wish to proceed anyway? (y/n) [n] y
```

9. Copie la configuración básica guardada anteriormente en la configuración de inicio.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Reinicie el conmutador:

```
switch# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

11. Cuando se pueda volver a acceder a la dirección IP de administración, inicie sesión en el switch a través de SSH.

Es posible que necesite actualizar las entradas del archivo host relacionadas con las claves SSH.

12. Copie el RCF al bootflash del switch CS1 usando 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 9000"](#) guías.

Muestra el ejemplo

Este ejemplo muestra que TFTP se está utilizando para copiar un RCF al bootflash en el switch CS1:

```
cs1# copy tftp: bootflash: vrf management  
Enter source filename: Nexus_9336C_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)...
```

13. 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 9000"](#) guías.

Muestra el ejemplo

En este ejemplo se muestra el archivo RCF Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt se está instalando en el interruptor cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands
```

14. Examine el resultado del banner desde el `show banner motd` comando. Debe leer y seguir estas instrucciones para asegurarse de que la configuración y el funcionamiento del interruptor son correctos.

Muestra el ejemplo

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date       : 10-23-2020
* Version    : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in confi
g mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

15. 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.

16. Vuelva a aplicar cualquier personalización anterior a la configuración del conmutador.
17. Después de comprobar que las versiones de RCF, las adiciones personalizadas y la configuración del switch son correctas, 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 9000"](#) guías.

```
cs1# copy running-config startup-config
```

```
[ ] 100% Copy complete
```

18. Reinicie el interruptor CS1. Puede ignorar las alertas de «monitor de estado del switch del clúster» y los eventos de «puertos inactivos» que se notifican en los nodos mientras se reinicia el switch.

```
cs1# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

19. 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 -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
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-01/cdp	e0a	cs1	Ethernet1/7	N9K-
C9336C	e0d	cs2	Ethernet1/7	N9K-
C9336C				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N9K-
C9336C	e0d	cs2	Ethernet1/8	N9K-
C9336C				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N9K-
C9336C	e0b	cs2	Ethernet1/1/1	N9K-
C9336C				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N9K-
C9336C	e0b	cs2	Ethernet1/1/2	N9K-
C9336C				

```
cluster1::*> system cluster-switch show -is-monitoring-enabled  
-operational true
```

Switch Model	Type	Address	
cs1	cluster-network	10.233.205.90	NX9-
C9336C			
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	NX9-

```

C9336C
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

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.

```

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 1 a 20 en el interruptor CS2.

22. Habilite la reversión automática en las LIF del clúster.

```

cluster1::*> network interface modify -vserver Cluster -lif * -auto-revert
True

```

Paso 3: Compruebe la configuración de la red del clúster y el estado del clúster

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
show interface brief
```

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 los nodos esperados siguen conectados:

```
show cdp neighbors
```

Muestra el ejemplo

```
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
cs1 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

Total entries displayed: 4

3. Compruebe que los nodos de clúster están en las VLAN de clúster correctas utilizando los siguientes comandos:

```
show vlan brief
```

```
show interface trunk
```

Muestra el ejemplo

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Eth1/1, Eth1/2, Eth1/3 Eth1/4, Eth1/5, Eth1/6, Eth1/7 Eth1/8, Eth1/35, Eth1/36 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
17	VLAN0017	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
18	VLAN0018	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
31	VLAN0031	active	Eth1/11, Eth1/12, Eth1/13 Eth1/14, Eth1/15, Eth1/16 Eth1/17, Eth1/18, Eth1/19 Eth1/20, Eth1/21, Eth1/22
32	VLAN0032	active	Eth1/23, Eth1/24, Eth1/25

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
Eth1/34

```

```
cs1# show interface trunk
```

```

-----
Port                Native  Status      Port
                   Vlan    Channel
-----
Eth1/1              1      trunking    --
Eth1/2              1      trunking    --
Eth1/3              1      trunking    --
Eth1/4              1      trunking    --
Eth1/5              1      trunking    --
Eth1/6              1      trunking    --
Eth1/7              1      trunking    --
Eth1/8              1      trunking    --
Eth1/9/1            1      trunking    --
Eth1/9/2            1      trunking    --
Eth1/9/3            1      trunking    --
Eth1/9/4            1      trunking    --
Eth1/10/1           1      trunking    --
Eth1/10/2           1      trunking    --
Eth1/10/3           1      trunking    --
Eth1/10/4           1      trunking    --
Eth1/11             33     trunking    --

```

Eth1/12	33	trunking	--
Eth1/13	33	trunking	--
Eth1/14	33	trunking	--
Eth1/15	33	trunking	--
Eth1/16	33	trunking	--
Eth1/17	33	trunking	--
Eth1/18	33	trunking	--
Eth1/19	33	trunking	--
Eth1/20	33	trunking	--
Eth1/21	33	trunking	--
Eth1/22	33	trunking	--
Eth1/23	34	trunking	--
Eth1/24	34	trunking	--
Eth1/25	34	trunking	--
Eth1/26	34	trunking	--
Eth1/27	34	trunking	--
Eth1/28	34	trunking	--
Eth1/29	34	trunking	--
Eth1/30	34	trunking	--
Eth1/31	34	trunking	--
Eth1/32	34	trunking	--
Eth1/33	34	trunking	--
Eth1/34	34	trunking	--
Eth1/35	1	trnk-bndl	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	1	trunking	--

```

-----
Port                Vlans Allowed on Trunk
-----
Eth1/1              1,17-18
Eth1/2              1,17-18
Eth1/3              1,17-18
Eth1/4              1,17-18
Eth1/5              1,17-18
Eth1/6              1,17-18
Eth1/7              1,17-18
Eth1/8              1,17-18
Eth1/9/1            1,17-18
Eth1/9/2            1,17-18
Eth1/9/3            1,17-18
Eth1/9/4            1,17-18
Eth1/10/1           1,17-18
Eth1/10/2           1,17-18
Eth1/10/3           1,17-18
Eth1/10/4           1,17-18

```

```

Eth1/11      31,33
Eth1/12      31,33
Eth1/13      31,33
Eth1/14      31,33
Eth1/15      31,33
Eth1/16      31,33
Eth1/17      31,33
Eth1/18      31,33
Eth1/19      31,33
Eth1/20      31,33
Eth1/21      31,33
Eth1/22      31,33
Eth1/23      32,34
Eth1/24      32,34
Eth1/25      32,34
Eth1/26      32,34
Eth1/27      32,34
Eth1/28      32,34
Eth1/29      32,34
Eth1/30      32,34
Eth1/31      32,34
Eth1/32      32,34
Eth1/33      32,34
Eth1/34      32,34
Eth1/35      1
Eth1/36      1
Po1          1
..
..
..
..
..

```



Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

4. 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      Pol (SU)      Eth      LACP      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

5. 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 LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

```
network interface revert -vserver vservice_name -lif lif_name
```

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					

node1					
	3/5/2022 19:21:18 -06:00		cluster1-01_clus2		cluster1-02-
clus1	none				
	3/5/2022 19:21:20 -06:00		cluster1-01_clus2		cluster1-
02_clus2	none				
node2					
	3/5/2022 19:21:18 -06:00		cluster1-02_clus2		cluster1-
01_clus1	none				
	3/5/2022 19:21:20 -06:00		cluster1-02_clus2		cluster1-
01_clus2	none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

El futuro

["Configure la supervisión de estado del switch".](#)

Restablecer el conmutador compartido 9336C-FX2 a los valores predeterminados de fábrica

Para restablecer el conmutador compartido 9336C-FX2 a los valores predeterminados de

fábrica, debe borrar la configuración del conmutador 9336C-FX2.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Borrar la configuración existente:

```
write erase
```

```
(cs2)# write erase
```

```
Warning: This command will erase the startup-configuration.  
Do you wish to proceed anyway? (y/n) [n] y
```

2. Recargue el software del conmutador:

```
reload
```

```
(cs2)# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

El sistema se reinicia y entra en el asistente de configuración. Durante el arranque, si recibe el mensaje “¿Desea cancelar el aprovisionamiento automático y continuar con la configuración normal?” (sí/no)[n]”, debe responder **sí** para continuar.

Migrar switches

Migre desde un clúster sin switches con almacenamiento de conexión directa

Puede migrar desde un clúster sin switches con almacenamiento de conexión directa añadiendo dos nuevos switches compartidos.

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 Twinax, pero no es compatible con este switch si los nodos utilizan puertos RJ45 DE 10 GB BASE-T integrados para los puertos de red del clúster.

La mayoría de los sistemas requieren dos puertos de red de clúster dedicados en cada controladora. Consulte ["Switches Ethernet de Cisco"](#) si quiere más información.

Si ya tiene un entorno de clúster sin switches de dos nodos, puede migrar a un entorno de clústeres con switches de dos nodos mediante switches Cisco Nexus 9336C-FX2 para permitirle escalar más allá de dos nodos del clúster.

Revise los requisitos

Asegúrese de que:

- Para la configuración de dos nodos sin switch:
 - La configuración sin switch de dos nodos está correctamente configurada y funciona.
 - Los nodos ejecutan ONTAP 9.8 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 **home**.
- Para la configuración de switches Cisco Nexus 9336C-FX2:
 - Ambos switches tienen conectividad de red de gestión.
 - Hay acceso de la consola a los switches de clúster.
 - Las conexiones de switch nodo a nodo y de switch a switch Nexus 9336C-FX2 utilizan cables Twinax o de fibra.
 - La solución de NetApp "[Hardware Universe](#)" contiene más información sobre el cableado.
 - Los cables de enlace entre switches (ISL) están conectados a los puertos 1/35 y 1/36 en los dos switches 9336C-FX2.
- Se ha completado la personalización inicial de los switches 9336C-FX2. Para que:
 - Los switches 9336C-FX2 ejecutan la versión más reciente del software
 - Los archivos de configuración de referencia (RCF) se han aplicado a los conmutadores
 - Cualquier personalización del sitio, como SMTP, SNMP y SSH, se configura en los nuevos switches.

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 conmutadores 9336C-FX2 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.
- El símbolo del sistema `cluster1:*>` indica el nombre del clúster.
- Los puertos de clúster que se utilizan en este procedimiento son *e3a* y *e3b*, como se indica en la controladora AFF A400. La "[Hardware Universe](#)" contiene la información más reciente acerca de los puertos del clúster reales para las plataformas.

Paso 1: Migrar desde un clúster sin switch con conexión directa

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.

1. cambie el nivel de privilegio a avanzado, introduciendo y cuando se le solicite continuar:

```
set -privilege advanced
```

Aparece el mensaje avanzado (*>).

2. 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 34 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 e1/1-34  
cs1(config-if-range)# shutdown
```

3. Compruebe que el ISL y los puertos físicos del ISL entre los dos switches 9336C-FX2 cs1 y cs2 estén activos en los puertos 1/35 y 1/36:

```
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      Eth1/35 (P)  Eth1/36 (P)
```

El siguiente ejemplo muestra que los puertos ISL están activos en el switch 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      Eth1/35 (P)  Eth1/36 (P)
```

4. 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               Eth1/35      175    R S I s         N9K-C9336C
Eth1/35
cs2               Eth1/36      175    R S I s         N9K-C9336C
Eth1/36
Total entries displayed: 2
```

En el siguiente ejemplo se enumeran 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               Eth1/35      177    R S I s         N9K-C9336C
Eth1/35
cs1               ) Eth1/36      177    R S I s         N9K-C9336C
Eth1/36
Total entries displayed: 2
```

5. Compruebe que todos los puertos del clúster estén activos:

```
network port show - ipspace Cluster
```

Cada puerto debe aparecer en enlace y en buen estado para Estado de salud.

Muestra el ejemplo

```
cluster1::*> network port show -ipspace Cluster
```

```
Node: node1
```

Health					Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy						
e3b	Cluster	Cluster		up	9000	auto/100000
healthy						

```
Node: node2
```

Health					Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy						
e3b	Cluster	Cluster		up	9000	auto/100000
healthy						

```
4 entries were displayed.
```

6. 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 tener un administrador de estado/Oper de up/up.

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
e3a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e3b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e3a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e3b	true			

4 entries were displayed.

7. 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.

8. desconecte el cable del puerto del clúster e3a del nodo 1 y, a continuación, conecte e3a al puerto 1 del switch del clúster cs1, utilizando el cableado adecuado admitido por los switches 9336C-FX2.

La solución de NetApp "[Hardware Universe](#)" contiene más información sobre el cableado.

9. Desconecte el cable del puerto del clúster e3a en el nodo 2 y, a continuación, conecte e3a al puerto 2 del

switch del clúster cs1, utilizando el cableado adecuado compatible con los switches 9336C-FX2.

10. 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 1/34 están habilitados en el conmutador cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-34
cs1(config-if-range)# no shutdown
```

11. Compruebe que todas las LIF de clúster están **up**, operativas y aparezcan como true para Is Home:

```
network interface show - vserver Cluster
```

Muestra el ejemplo

En el ejemplo siguiente se muestra que todas las LIF están **up** en los nodos 1 y 2 y eso es Is Home los resultados son **true**:

```
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	e3a
true	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true	node2_clus1	up/up	169.254.47.194/16	node2	e3a
true	node2_clus2	up/up	169.254.19.183/16	node2	e3b
4 entries were displayed.					

12. muestra información sobre el estado de los nodos del 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.
```

13. desconecte el cable del puerto del clúster e3b en el nodo 1 y, a continuación, conecte e3b al puerto 1 del switch de clúster cs2 con el cableado adecuado compatible con los switches 9336C-FX2.
14. Desconecte el cable del puerto de clúster e3b en el nodo 2 y, a continuación, conecte e3b al puerto 2 del switch de clúster cs2 con el cableado adecuado compatible con los switches 9336C-FX2.
15. 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 1/34 están habilitados en el conmutador cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-34
cs2(config-if-range)# no shutdown
```

16. 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

Health	Health				Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	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					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

4 entries were displayed.

17. Compruebe que todas las interfaces se muestran como verdaderas 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 **up** 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	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e3a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e3b
true					
4 entries were displayed.					

18. Compruebe que ambos nodos tienen cada uno una conexión a 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         Local Intrfce  Hldtme  Capability  Platform
Port ID
node1             Eth1/1        133     H           AFFA400
e3a
node2             Eth1/2        133     H           AFFA400
e3a
cs2               Eth1/35       175     R S I s     N9K-C9336C
Eth1/35
cs2               Eth1/36       175     R S I s     N9K-C9336C
Eth1/36
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         Local Intrfce  Hldtme  Capability  Platform
Port ID
node1             Eth1/1        133     H           AFFA400
e3b
node2             Eth1/2        133     H           AFFA400
e3b
cs1               Eth1/35       175     R S I s     N9K-C9336C
Eth1/35
cs1               Eth1/36       175     R S I s     N9K-C9336C
Eth1/36
Total entries displayed: 4
```

19. Mostrar 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
           e3a    cs1                      0/2          N9K-
C9336C
           e3b    cs2                      0/2          N9K-
C9336C
node1      /cdp
           e3a    cs1                      0/1          N9K-
C9336C
           e3b    cs2                      0/1          N9K-
C9336C
4 entries were displayed.
```

20. Compruebe que la configuración del almacenamiento del par de alta disponibilidad 1 (y del par de alta disponibilidad 2) sea correcta y esté libre de errores:

```
system switch ethernet show
```

Muestra el ejemplo

```
storage::*> system switch ethernet show
Switch                                     Type                               Address
Model
-----
sh1
                                     storage-network                     172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
sh2
                                     storage-network                     172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
2 entries were displayed.
storage::*>
```

21. Compruebe que los ajustes están desactivados:

```
network options switchless-cluster show
```



El comando puede tardar varios minutos en completarse. Espere a que se anuncie la duración de 3 minutos.

La *false* el resultado del ejemplo siguiente muestra que las opciones de configuración están deshabilitadas:

Muestra el ejemplo

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

22. 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

23. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
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)

```

1. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

Paso 2: Configurar el conmutador compartido

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos conmutadores compartidos son *sh1* y *sh2*.
- Los nodos son *1* y *2*.



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.

1. Compruebe que la configuración del almacenamiento de la pareja de alta disponibilidad 1 (y par de alta disponibilidad 2) sea correcta y esté libre de errores:

```
system switch ethernet show
```

Muestra el ejemplo

```
storage::*> system switch ethernet show
Switch                                     Type                                     Address
Model
-----
sh1
                                     storage-network                             172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
sh2
                                     storage-network                             172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
2 entries were displayed.
storage::*>
```

2. Compruebe que los puertos del nodo de almacenamiento estén en buen estado y estén operativos:

```
storage port show -port-type ENET
```

Muestra el ejemplo

```
storage::*> storage port show -port-type ENET
```

				Speed		
VLAN	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online

3. mueva el par ha 1, NSM224 ruta a puertos a la gama de puertos sh1 11-22.
4. Instale un cable desde el par ha 1, el nodo 1, la ruta A hasta el puerto sh1 de rango 11-22. Por ejemplo, la ruta de Un puerto de almacenamiento de un AFF A400 es e0c.
5. Instale un cable del par de alta disponibilidad 1, 2, ruta A al intervalo de puertos sh1 11-22.
6. 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
```

				Speed		
VLAN	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	0	enabled	offline
30	e5a	ENET	storage	0	enabled	offline
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	0	enabled	offline
30	e5a	ENET	storage	0	enabled	offline
30	e5b	ENET	storage	100	enabled	online

7. Compruebe 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.

8. Mueva los puertos de la ruta B del par de alta disponibilidad 1 y NSM224 al intervalo de puertos sh2 11-22.
9. Instale un cable desde el par de alta disponibilidad 1, el nodo 1, la ruta B hasta el puerto sh2 del rango 11-22. Por ejemplo, el puerto de almacenamiento de la ruta B de un AFF A400 es e5b.
10. Instale un cable del par de alta disponibilidad 1, 2, ruta B al intervalo de puertos sh2 11-22.

11. 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	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	0	enabled	offline
30	e5a	ENET	storage	0	enabled	offline
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	0	enabled	offline
30	e5a	ENET	storage	0	enabled	offline
30	e5b	ENET	storage	100	enabled	online

12. Compruebe que la configuración del almacenamiento del par de alta disponibilidad 1 sea correcta y esté libre de errores:

```
system switch ethernet show
```

Muestra el ejemplo

```
storage::*> system switch ethernet show
Switch                                     Type                               Address
Model
-----
sh1
                                     storage-network                172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
sh2
                                     storage-network                172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
2 entries were displayed.
storage::*>
```

13. Vuelva a configurar los puertos de almacenamiento secundario no utilizados (controladora) en el par de alta disponibilidad 1 del almacenamiento a la red. Si se ha conectado directamente a más de un NS224, habrá puertos que volver a configurar.

Muestra el ejemplo

```
storage port modify -node [node name] -port [port name] -mode
network
```

Para colocar puertos de almacenamiento en un dominio de retransmisión:

- ° network port broadcast-domain create (para crear un nuevo dominio, si es necesario)

- `network port broadcast-domain add-ports` (para agregar puertos a un dominio existente)

14. 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
```

El futuro

"Configure la supervisión de estado del switch".

Migrar desde una configuración conmutada con almacenamiento de conexión directa

Puede migrar desde una configuración con switch con almacenamiento de conexión directa agregando dos nuevos switches compartidos.

Switches compatibles

Se admiten los siguientes switches:

- Nexus 9336C-FX2
- Nexus 3232C

Las versiones ONTAP y NX-OS compatibles con este procedimiento se encuentran en la página Cisco Ethernet Switches. Consulte "[Switches Ethernet de Cisco](#)".

Puertos de conexión

Los switches utilizan los siguientes puertos para conectarse a los nodos:

- Nexus 9336C-FX2:
 - Puertos 1- 3: Modo de arranque (4 x 10 G) puertos intra-clúster, int e1/1/1-4, e1/2/1-4, e1/3/1-4
 - Puertos 4- 6: Modo de arranque (4x25G) puertos Intra-Cluster/ha, int e1/4/1-4, e1/5/1-4, e1/6/1-4
 - Puertos 7-34: Puertos intra-clúster/alta disponibilidad de 40 GbE, int e1/7-34
- Nexus 3232C:
 - Puertos 1-30: 10/40/100 GbE
- Los switches utilizan los siguientes puertos de enlace entre switches (ISL):
 - Puertos E1/35-36: Nexus 9336C-FX2
 - Puertos e1/31-32: Nexus 3232C

La "[Hardware Universe](#)" contiene información sobre el cableado compatible para todos los switches de clúster.

Lo que necesitará

- Asegúrese de completar las siguientes tareas:
 - Se configuraron algunos puertos en los switches Nexus 9336C-FX2 a 100 GbE.
 - Conectividad 100 GbE planificada, migrada y documentada desde nodos a switches Nexus 9336C-FX2.
 - Migre de forma no disruptiva otros switches de clúster Cisco de un clúster ONTAP a los switches de red Cisco Nexus 9336C-FX2.
- La red de switches existente está correctamente configurada y funciona.

- Todos los puertos se encuentran en el estado **up** para garantizar operaciones no disruptivas.
- Los switches Nexus 9336C-FX2 están configurados y funcionan con la versión adecuada del archivo de configuración de referencia (RCF) y de NX-OS instalado.
- La configuración de red existente tiene lo siguiente:
 - 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.
 - Todas las LIF del clúster en el estado **up** con las LIF del clúster se encuentran en sus puertos de inicio.
 - Puertos ISL habilitados y cableado entre los otros switches Cisco y entre los nuevos switches.

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 3232C son *c1* y *c2*.
- Los nuevos switches Nexus 9336C-FX2 son *sh1* y *sh2*.
- 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 *sh2* y, a continuación, el interruptor *c1* se sustituye por el interruptor *sh1*.

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.

2. Compruebe el estado administrativo y operativo de cada puerto del clúster.
3. 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: node1

Ignore
Speed (Mbps)  Health
Health
Port    IPspace  Broadcast Domain Link MTU  Admin/Ope  Status
Status
-----
-----
e3a     Cluster  Cluster          up   9000  auto/100000 healthy
false
e3b     Cluster  Cluster          up   9000  auto/100000 healthy
false

Node: node2

Ignore
Speed (Mbps)  Health
Health
Port    IPspace  Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e3a     Cluster  Cluster          up   9000  auto/100000 healthy
false
e3b     Cluster  Cluster          up   9000  auto/100000 healthy
false
4 entries were displayed.
cluster1::*>
```

4. Compruebe que todas las interfaces de clúster (LIF) estén en el 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					
node1_clus1	up/up	169.254.3.4/23	node1	e3a	
true					
node1_clus2	up/up	169.254.3.5/23	node1	e3b	
true					
node2_clus1	up/up	169.254.3.8/23	node2	e3a	
true					
node2_clus2	up/up	169.254.3.9/23	node2	e3b	
true					
4 entries were displayed.					
cluster1::*>					

5. Compruebe que el clúster muestre información de los dos switches del 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
sh1	cluster-network	10.233.205.90	N9K-
C9336C			
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
sh2	cluster-network	10.233.205.91	N9K-
C9336C			
Serial Number: FOCXXXXXXGS			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			

```
cluster1::*>
```

6. deshabilite la reversión automática en las LIF del clúster.

Muestra el ejemplo

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto  
-revert false
```

7. apague el interruptor c2.

Muestra el ejemplo

```
c2# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
c2(config)# interface ethernet <int range>  
c2(config)# shutdown
```


8. Compruebe que las LIF del clúster han migrado a los puertos alojados en el switch del clúster sh1:

```
network interface show -role cluster
```

Esto puede tardar unos segundos.

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					
	node1_clus1	up/up	169.254.3.4/23	node1	e3a
true					
	node1_clus2	up/up	169.254.3.5/23	node1	e3a
false					
	node2_clus1	up/up	169.254.3.8/23	node2	e3a
true					
	node2_clus2	up/up	169.254.3.9/23	node2	e3a
false					
4 entries were displayed.					
cluster1::*>					

9. sustituya el interruptor c2 por el nuevo interruptor sh2 y vuelva a conectar el nuevo interruptor.
10. Compruebe que los puertos están de nuevo en sh2. **Tenga en cuenta** que los LIF siguen en el conmutador c1.
11. Apague el interruptor c1.

Muestra el ejemplo

```
c1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c1(config)# interface ethernet <int range>
c1(config)# shutdown
```

12. [[paso 12]] Compruebe que las LIF del clúster han migrado a los puertos alojados en el switch del clúster sh2. Esto puede tardar unos segundos.

Muestra el ejemplo

```
cluster1::*> network interface show -role cluster
```

Is	Logical	Status	Network	Current	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----

Cluster					
true	node1_clus1	up/up	169.254.3.4/23	node1	e3a
false	node1_clus2	up/up	169.254.3.5/23	node1	e3a
true	node2_clus1	up/up	169.254.3.8/23	node2	e3a
false	node2_clus2	up/up	169.254.3.9/23	node2	e3a

4 entries were displayed.
cluster1::*>

- sustituya el interruptor c1 por el nuevo interruptor sh1 y vuelva a conectar el nuevo interruptor.
- Compruebe que los puertos están de nuevo en sh1. **Nota** que los LIF están todavía en el conmutador c2.
- Habilite la reversión automática en las LIF del clúster:

Muestra el ejemplo

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto  
-revert True
```

- Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

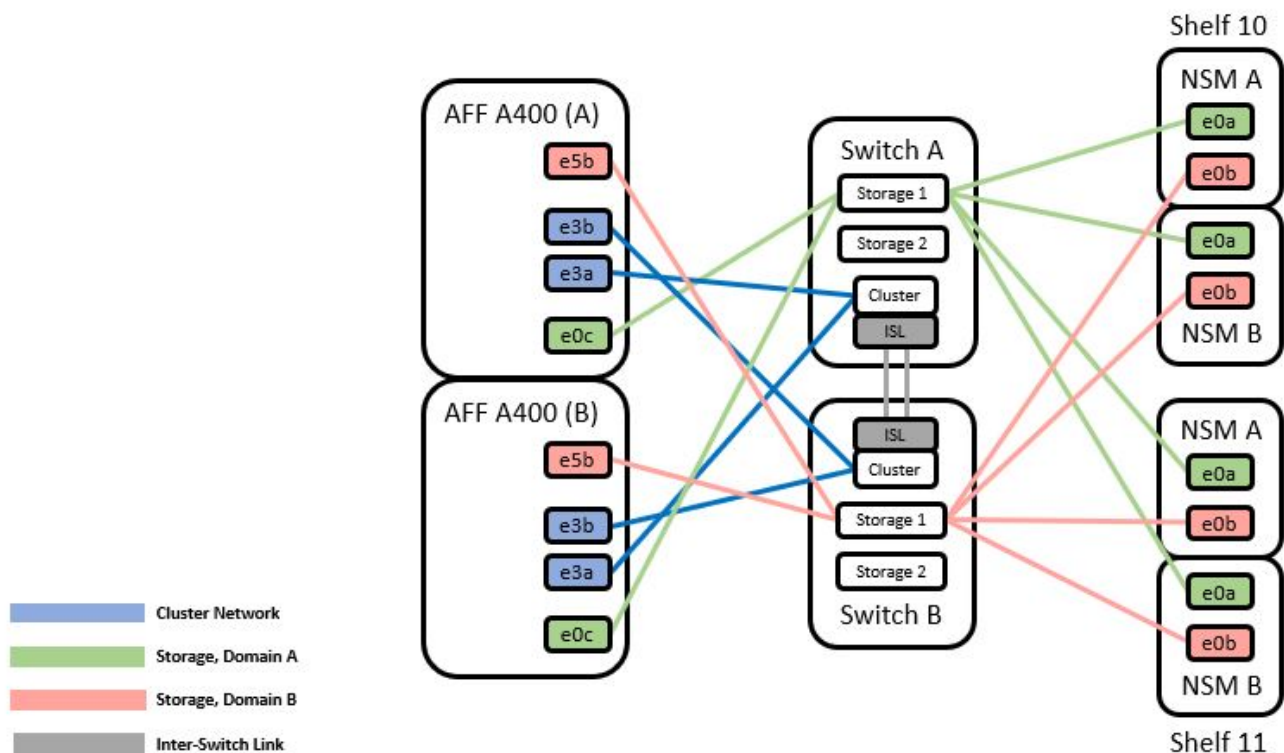
```
cluster1::*> cluster show
Node           Health Eligibility Epsilon
-----
node1          true   true      false
node2          true   true      false
2 entries were displayed.
cluster1::*>
```

Migre de una configuración sin switches con almacenamiento conectado mediante la reutilización de los switches de almacenamiento

Puede migrar desde una configuración sin switches con almacenamiento conectado a switches reutilizando los switches de almacenamiento.

Mediante la reutilización de los switches de almacenamiento, los switches de almacenamiento del par de alta disponibilidad 1 se convierten en los switches compartidos, como se muestra en la siguiente figura.

Switch Attached



Pasos

1. Compruebe que la configuración del almacenamiento de la pareja de alta disponibilidad 1 (y par de alta disponibilidad 2) sea correcta y esté libre de errores:

```
system switch ethernet show
```

Muestra el ejemplo

```
storage::*> system switch ethernet show
Switch                                     Type                               Address
Model
-----
sh1
                                     storage-network                     172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: none
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
sh2
                                     storage-network                     172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
2 entries were displayed.
storage::*>
```

2. Compruebe que los puertos del nodo estén en buen estado y operativos:

```
storage port show -port-type ENET
```

Muestra el ejemplo

```
storage::*> storage port show -port-type ENET
```

				Speed		
VLAN	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online

3. mueva Los cables de la ruta A del par de alta disponibilidad 1, NSM224, desde el switch de almacenamiento A hasta los puertos de almacenamiento compartidos NS224 para el par de alta disponibilidad 1, ruta A en el switch de almacenamiento A.
4. Mueva el cable de la ruta A del par de alta disponibilidad 1, nodo A, al puerto de almacenamiento compartido para el par de alta disponibilidad 1, nodo A en el switch de almacenamiento A.
5. Mueva el cable de la ruta A del par de alta disponibilidad 1, nodo B, al puerto de almacenamiento compartido para el par de alta disponibilidad 1, nodo B en el switch de almacenamiento A.
6. Compruebe que el almacenamiento conectado al par de alta disponibilidad 1, el switch De almacenamiento A sea correcto:

```
system health alert show -instance
```

Muestra el ejemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

7. sustituya el RCF de almacenamiento en el conmutador compartido A por el archivo RCF compartido. Consulte ["Instale el RCF en un switch compartido Cisco Nexus 9336C-FX2"](#) para obtener más detalles.
8. Compruebe que el almacenamiento conectado al par de alta disponibilidad 1, el switch de almacenamiento B sea correcto:

```
system health alert show -instance
```

Muestra el ejemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

9. mueva los cables de la ruta B del par de alta disponibilidad 1 y NSM224 del conmutador de almacenamiento B a los puertos de almacenamiento compartidos NS224 para el par de alta disponibilidad 1, ruta B al conmutador de almacenamiento B.
10. Mueva el cable desde el par de alta disponibilidad 1, nodo A, ruta B al puerto de almacenamiento compartido para el par de alta disponibilidad 1, nodo A, ruta B en el switch de almacenamiento B.
11. Mueva el cable desde el par de alta disponibilidad 1, nodo B, ruta B al puerto de almacenamiento compartido para el par de alta disponibilidad 1, nodo B, ruta B en el switch de almacenamiento B.
12. Compruebe que el almacenamiento conectado al par de alta disponibilidad 1, el switch de almacenamiento B sea correcto:

```
system health alert show -instance
```

Muestra el ejemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

13. sustituya el archivo RCF de almacenamiento en el conmutador compartido B por el archivo RCF compartido. Consulte ["Instale el RCF en un switch compartido Cisco Nexus 9336C-FX2"](#) para obtener más detalles.
14. Compruebe que el almacenamiento conectado al par de alta disponibilidad 1, el switch de almacenamiento B sea correcto:

```
system health alert show -instance
```

Muestra el ejemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

15. instale los ISL entre el switch compartido A y el conmutador compartido B:

Muestra el ejemplo

```
sh1# configure  
Enter configuration commands, one per line. End with CNTL/Z.  
sh1 (config)# interface e1/35-36  
sh1 (config-if-range)# no lldp transmit  
sh1 (config-if-range)# no lldp receive  
sh1 (config-if-range)# switchport mode trunk  
sh1 (config-if-range)# no spanning-tree bpduguard enable  
sh1 (config-if-range)# channel-group 101 mode active  
sh1 (config-if-range)# exit  
sh1 (config)# interface port-channel 101  
sh1 (config-if)# switchport mode trunk  
sh1 (config-if)# spanning-tree port type network  
sh1 (config-if)# exit  
sh1 (config)# exit
```

16. convierta el par de alta disponibilidad 1 de un clúster sin switches a un clúster con switches. Utilice las asignaciones de puertos del clúster definidas por el RCF compartido. Consulte ["Instalar el software NX-OS y los archivos de configuración de referencia \(RCF\)"](#) para obtener más detalles.
17. Compruebe que la configuración de red conmutada sea válida:

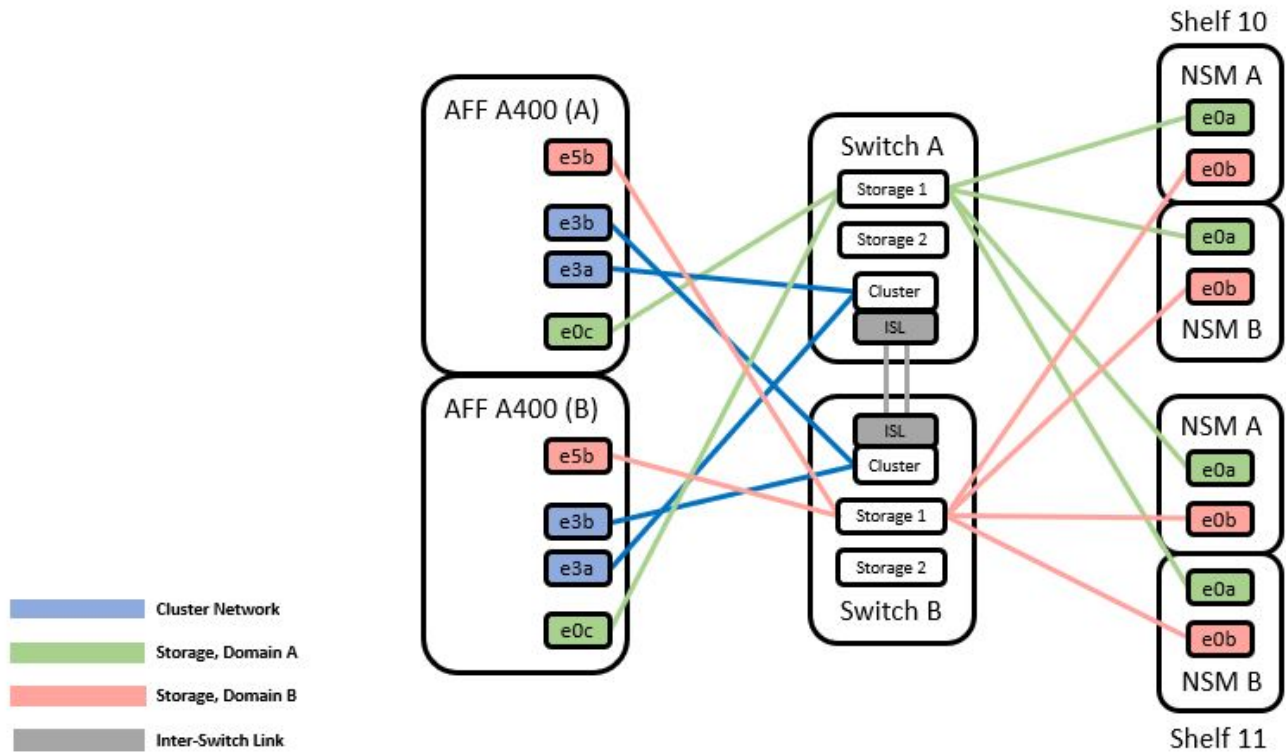
```
network port show
```

Migre desde un clúster con switches con almacenamiento conectado a switches

Puede migrar desde un clúster conmutado con almacenamiento conectado a switches reutilizando los switches de almacenamiento.

Mediante la reutilización de los switches de almacenamiento, los switches de almacenamiento del par de alta disponibilidad 1 se convierten en los switches compartidos, como se muestra en la siguiente figura.

Switch Attached



Pasos

1. Compruebe que la configuración del almacenamiento de la pareja de alta disponibilidad 1 (y par de alta disponibilidad 2) sea correcta y esté libre de errores:

```
system switch ethernet show
```


Muestra el ejemplo

```
storage::*> system switch ethernet show
```

Switch	Type	Address	Model

sh1	storage-network	172.17.227.5	C9336C
Serial Number: FOC221206C2			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
sh2	storage-network	172.17.227.6	C9336C
Serial Number: FOC220443LZ			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
2 entries were displayed.			

```
storage::*>
```

2. mueva Los cables de la ruta A del par de alta disponibilidad 1, NSM224 de la ruta A del switch de almacenamiento a a los puertos de almacenamiento NSM224 para el par de alta disponibilidad 1, ruta A en el conmutador de almacenamiento A.
3. Mueva el cable desde el par de alta disponibilidad 1, nodo A, ruta A al puerto de almacenamiento NSM224 para el par de alta disponibilidad 1, nodo A en el switch de almacenamiento A.
4. Mueva el cable desde el par de alta disponibilidad 1, nodo B, ruta A al puerto de almacenamiento NSM224 para el par de alta disponibilidad 1, nodo B en el switch de almacenamiento A.
5. Compruebe que el almacenamiento conectado al par de alta disponibilidad 1, el switch De almacenamiento A sea correcto:

```
storage port show -port-type ENET
```

Muestra el ejemplo

```
storage::*> storage port show -port-type ENET
```

				Speed		
VLAN	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online

- sustituya el RCF de almacenamiento en el conmutador compartido A por el archivo RCF compartido. Consulte ["Instale el RCF en un switch compartido Cisco Nexus 9336C-FX2"](#) para obtener más detalles.
- Compruebe que el almacenamiento conectado al par de alta disponibilidad 1, el switch De almacenamiento A sea correcto:

```
system health alert show -instance
```

Muestra el ejemplo

```
storage::*> system health alert show -instance
```

There are no entries matching your query.

- mueva los cables de la ruta B del par de alta disponibilidad 1 y NSM224 del conmutador de almacenamiento B a los puertos de almacenamiento compartidos NS224 para el par de alta disponibilidad

1, ruta B al conmutador de almacenamiento B.

9. Mueva el cable desde el par de alta disponibilidad 1, nodo A, ruta B al puerto de almacenamiento compartido para el par de alta disponibilidad 1, nodo A, ruta B en el switch de almacenamiento B.
10. Mueva el cable desde el par de alta disponibilidad 1, nodo B, ruta B al puerto de almacenamiento compartido para el par de alta disponibilidad 1, nodo B, ruta B en el switch de almacenamiento B.
11. Compruebe que el almacenamiento conectado al par de alta disponibilidad 1, el switch de almacenamiento B sea correcto:

```
system health alert show -instance
```

Muestra el ejemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

12. sustituya el archivo RCF de almacenamiento en el conmutador compartido B por el archivo RCF compartido. Consulte ["Instale el RCF en un switch compartido Cisco Nexus 9336C-FX2"](#) para obtener más detalles.
13. Compruebe que el almacenamiento conectado al par de alta disponibilidad 1, el switch de almacenamiento B sea correcto:

```
system health alert show -instance
```

Muestra el ejemplo

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

14. Verifique que la configuración de almacenamiento del par de alta disponibilidad 1 sea correcta y no tenga errores:

```
system switch ethernet show
```

Muestra el ejemplo

```
storage::*> system switch ethernet show
```

Switch	Type	Address
sh1	storage-network	172.17.227.5
C9336C		
Serial Number: FOC221206C2		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version		
9.3(5)		
Version Source: CDP		
sh2	storage-network	172.17.227.6
C9336C		
Serial Number: FOC220443LZ		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version		
9.3(5)		
Version Source: CDP		
2 entries were displayed.		

```
storage::*>
```

15. instale los ISL entre el switch compartido A y el conmutador compartido B:

Muestra el ejemplo

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config)# interface e1/35-36*
sh1 (config-if-range)# no lldp transmit
sh1 (config-if-range)# no lldp receive
sh1 (config-if-range)# switchport mode trunk
sh1 (config-if-range)# no spanning-tree bpduguard enable
sh1 (config-if-range)# channel-group 101 mode active
sh1 (config-if-range)# exit
sh1 (config)# interface port-channel 101
sh1 (config-if)# switchport mode trunk
sh1 (config-if)# spanning-tree port type network
sh1 (config-if)# exit
sh1 (config)# exit
```

16. migre la red del clúster desde los switches del clúster existentes a los switches compartidos mediante el procedimiento de sustitución del switch y el RCF compartido. El nuevo conmutador compartido A es "cs1". El nuevo conmutador compartido B es "cs2". Consulte ["Sustituya un switch compartido Cisco Nexus 9336C-FX2"](#) y.. ["Instale el RCF en un switch compartido Cisco Nexus 9336C-FX2"](#) para obtener más detalles.
17. Compruebe que la configuración de red conmutada sea válida:

```
network port show
```

18. Quite los switches de clúster que no se utilicen.
19. Retire los interruptores de almacenamiento que no se utilicen.

Sustituya un switch compartido Cisco Nexus 9336C-FX2

Puede sustituir un conmutador compartido Nexus 9336C-FX2 defectuoso. Este es un procedimiento no disruptivo (NDU).

Antes de empezar

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 son **up**.
 - Todas las interfaces lógicas de cluster (LIF) son **up** y en sus puertos domésticos.
 - 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 9336C-FX2:

- 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 1/34:
- Todos los puertos de enlace entre switches (ISL) están deshabilitados en los puertos 1/35 y 1/36.
- El archivo de configuración de referencia (RCF) y el conmutador de imagen del sistema operativo NX-OS se cargan en el conmutador.
- Cualquier personalización de sitio anterior, como STP, SNMP y SSH, se debe copiar al nuevo switch.

Acerca de los ejemplos

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 nomenclatura de conmutador y nodo siguiente:

- Los nombres de los switches Nexus 9336C-FX2 existentes son *sh1* y *sh2*.
- El nombre de los nuevos switches Nexus 9336C-FX2 es *newsh1* y *newsh2*.
- Los nombres de nodo son *1* y *2*.
- Los puertos de clúster de cada nodo se denominan *e3a* y *e3b*.
- 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 símbolo del sistema de cambios en todos los nodos del cluster es *cluster1:*>*.



El siguiente procedimiento se basa en la siguiente topología de red:

Mostrar topología de ejemplo

cluster1::*> network port show -ipspace Cluster

Node: node1

Ignore						
						Speed(Mbps)
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						Status

e3a	Cluster	Cluster		up	9000	auto/100000
false						healthy
e3b	Cluster	Cluster		up	9000	auto/100000
false						healthy

Node: node2

Ignore						
						Speed(Mbps)
Health						
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						Status

e3a	Cluster	Cluster		up	9000	auto/100000
false						healthy
e3b	Cluster	Cluster		up	9000	auto/100000
false						healthy

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	e3a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e3b
true					

```

node2_clus1 up/up 169.254.47.194/16 node2 e3a
true
node2_clus2 up/up 169.254.19.183/16 node2 e3b
true
4 entries were displayed.

```

cluster1::*> **network device-discovery show -protocol cdp**

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e3a	sh1	Eth1/2	N9K-
C9336C				
	e3b	sh2	Eth1/2	N9K-
C9336C				
node1	/cdp			
	e3a	sh1	Eth1/1	N9K-
C9336C				
	e3b	sh2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

sh1# **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	e3a
node2	Eth1/2	145	H	FAS2980	e3a
sh2	Eth1/35	176	R S I s	N9K-C9336C	
Eth1/35					
sh2 (FDO220329V5)	Eth1/36	176	R S I s	N9K-C9336C	
Eth1/36					

Total entries displayed: 4

sh2# **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          139      H          FAS2980      eb
node2          Eth1/2          124      H          FAS2980      eb
sh1            Eth1/35         178      R S I s    N9K-C9336C
Eth1/35
sh1            Eth1/36         178      R S I s    N9K-C9336C
Eth1/36
Total entries displayed: 4

```

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.

2. Opcional: Instale el RCF y la imagen adecuados en el interruptor, news2, y realice los preparativos necesarios en el sitio.
 - a. 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 switch está correctamente configurado y no necesita actualizaciones para el software RCF y NX-OS, continúe con [Paso 3](#).
 - b. Vaya a la página NetApp Cluster and Management Network Switches Reference Configuration File Description en el sitio de soporte de NetApp.
 - c. Haga clic en el enlace de la matriz de compatibilidad de red de administración y red de clúster y, a continuación, anote la versión de software del switch que desee.
 - d. Haga clic en la flecha de retroceso del explorador para volver a la página Descripción, haga clic en CONTINUAR, acepte el acuerdo de licencia y, a continuación, vaya a la página Descargar.
 - e. 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.
3. en el nuevo switch, inicie sesión como administrador y apague todos los puertos que se conectarán a las interfaces del clúster de nodos (puertos 1/1 a 1/34). Si el interruptor que desea sustituir no funciona y está apagado, vaya a [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

```

newsh2# config
Enter configuration commands, one per line. End with CNTL/Z.
newsh2(config)# interface e1/1-34
newsh2(config-if-range)# shutdown

```

4. 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
```

	Logical	
Vserver	Interface	Auto-revert
-----	-----	-----
Cluster	node1_clus1	true
Cluster	node1_clus2	true
Cluster	node2_clus1	true
Cluster	node2_clus2	true

4 entries were displayed.

5. Verifique la conectividad de las interfaces del cluster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
none			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
none			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
none			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
none			

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
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)

```

1. cierre los puertos ISL 1/35 y 1/36 en el switch Nexus 9336C-FX2 sh1.

Muestra el ejemplo

```

sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1(config)# interface e1/35-36
sh1(config-if-range)# shutdown

```

2. retire todos los cables del conmutador Nexus 9336C-FX2 sh2 y, a continuación, conéctelos a los mismos puertos del conmutador Nexus C9336C-FX2 news2.
3. Traiga los puertos ISLs 1/35 y 1/36 entre los conmutadores sh1 y news2 y, a continuación, verifique el estado de funcionamiento del canal de puerto.

Port-Channel debe indicar PO1(su) y los puertos de miembro deben indicar eth1/35(P) y eth1/36(P).

Muestra el ejemplo

En este ejemplo se habilitan los puertos ISL 1/35 y 1/36 y se muestra el resumen del canal de puerto en el conmutador sh1.

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config)# int e1/35-36
sh1 (config-if-range)# no shutdown
sh1 (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       Eth1/35 (P)  Eth1/36 (P)

sh1 (config-if-range)#
```

4. Compruebe que el puerto e3b está activo en todos los nodos:

```
network port show ipspace Cluster
```

Muestra el ejemplo

La salida debe ser como 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
-----
e3a         Cluster      Cluster      up    9000    auto/100000
healthy     false
e3b         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
-----
e3a         Cluster      Cluster      up    9000    auto/100000
healthy     false
e3b         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 de clúster asociada con el puerto en el paso anterior utilizando el comando `network interface revert`.

En este ejemplo, la LIF `no1_clus2` del nodo 1 se revierte correctamente si el valor del Inicio es `TRUE` y el puerto es `e3b`.

Los siguientes comandos devuelven la LIF `no1_clus2` del nodo 1 al puerto de inicio `e3a` y muestran información acerca de las LIF de ambos nodos. La creación del primer nodo se realiza correctamente si la columna `is Home` es **true** para ambas interfaces de clúster y muestran las asignaciones de puertos correctas, en este ejemplo `e3a` y `e3b` en el nodo 1.

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				
e3a	node1_clus1	up/up	169.254.209.69/16	node1
	true			
e3b	node1_clus2	up/up	169.254.49.125/16	node1
	true			
e3a	node2_clus1	up/up	169.254.47.194/16	node2
	true			
e3a	node2_clus2	up/up	169.254.19.183/16	node2
	false			
4 entries were displayed.				

6. Mostrar 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 activos:

```
network port show ipspace Cluster
```

Muestra el ejemplo

```
cluster1::*> network port show -ipspace Cluster
```

Node node1

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----			-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

						Speed (Mbps)
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					
4 entries were displayed.						

8. Verifique la conectividad de las interfaces del cluster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
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)

```

1. 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					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

		Speed (Mbps)				
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
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	
e3a	true				
	node1_clus2	up/up	169.254.49.125/16	node1	
e3b	true				
	node2_clus1	up/up	169.254.47.194/16	node2	

```
e3a      true
          node2_clus2  up/up      169.254.19.183/16  node2
```

```
e3b      true
```

```
4 entries were displayed.
```

```
cluster1::> network device-discovery show -protocol cdp
```

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

node2	/cdp			
	e3a	sh1 0/2	N9K-C9336C	
	e3b	newsh2	0/2	N9K-
C9336C				
node1	/cdp			
	e3a	sh1	0/1	N9K-
C9336C				
	e3b	newsh2	0/1	N9K-
C9336C				

```
4 entries were displayed.
```

```
sh1# 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
e3a					
node2		Eth1/2	145	H	FAS2980
e3a					
newsh2		Eth1/35	176	R S I s	N9K-C9336C
Eth1/35					
newsh2		Eth1/36	176	R S I s	N9K-C9336C
Eth1/36					

```
Total entries displayed: 4
```

```
sh2# 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	139	H	FAS2980
e3b				
node2	Eth1/2	124	H	FAS2980
eb				
sh1	Eth1/35	178	R S I s	N9K-C9336C
Eth1/35				
sh1	Eth1/36	178	R S I s	N9K-C9336C
Eth1/36				
Total entries displayed: 4				

- mueva los puertos de almacenamiento del interruptor sh2 antiguo al nuevo interruptor news2.
- Compruebe que el almacenamiento conectado al par de alta disponibilidad 1 y que el switch compartido news2 esté en buen estado.
- Compruebe que el almacenamiento conectado al par de alta disponibilidad 2 y que el switch compartido news2 esté en buen estado:

```
storage port show -port-type ENET
```

Muestra el ejemplo

```
storage::*> storage port show -port-type ENET
```

VLAN				Speed		
Node	Port	Type	Mode	(Gb/s)	State	Status
ID						

node1						
30	e3a	ENET	storage	100	enabled	online
30	e3b	ENET	storage	0	enabled	offline
30	e7a	ENET	storage	0	enabled	offline
30	e7b	ENET	storage	100	enabled	online
node2						
30	e3a	ENET	storage	100	enabled	online
30	e3b	ENET	storage	0	enabled	offline
30	e7a	ENET	storage	0	enabled	offline
30	e7b	ENET	storage	100	enabled	online

5. Compruebe que las estanterías estén cableadas correctamente:

```
storage shelf port show -fields remote- device,remote-port
```

Muestra el ejemplo

```
cluster1::*> storage shelf port show -fields remote-device,remote-  
port  
shelf id remote-port  remote-device  
----- --  
3.20  0  Ethernet1/13  sh1  
3.20  1  Ethernet1/13  newsh2  
3.20  2  Ethernet1/14  sh1  
3.20  3  Ethernet1/14  newsh2  
3.30  0  Ethernet1/15  sh1  
3.30  1  Ethernet1/15  newsh2  
3.30  2  Ethernet1/16  sh1  
3.30  3  Ethernet1/16  newsh2  
8 entries were displayed.
```

6. retire el interruptor sh2 antiguo.
7. Repita estos pasos para el interruptor sh1 y el interruptor nuevo1.
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
```

El futuro

"Configure la supervisión de estado del switch".

Supervise el estado del interruptor

Descripción general del monitor de estado del switch

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.

Configure la supervisión de estado del switch

Información general de configuración

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.

- ["Configure la recopilación de registros"](#)
- ["Opcional: Configure SNMPv3"](#)

Configure la recopilación de registros

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 de la recopilación, solicitando registros detallados de **Soporte** y habilitando una recopilación por hora de datos **Periódicos** que es recopilada por AutoSupport.

NOTA: Si habilita el modo FIPS, debe completar lo siguiente:



1. Vuelva a generar las claves SSH en el switch siguiendo las instrucciones del proveedor.
2. Regenerar claves SSH en ONTAP mediante `debug system regenerate-systemshell-key-pair`
3. Volver a ejecutar la rutina de configuración de la recogida de registros con `system switch ethernet log setup-password` el comando

Antes de empezar

- El usuario debe tener acceso a los comandos de cambio `show`. Si no están disponibles, cree un nuevo usuario y otorgue los permisos necesarios al usuario.
- 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.
- Para la recopilación de registros con switches Broadcom y Cisco:
 - El usuario local debe tener privilegios de administrador de red.

- Se debe crear un usuario nuevo en el switch de cada configuración del clúster con la recopilación de registros habilitada. Estos switches no admiten varias claves SSH para el mismo usuario. Cualquier configuración de recopilación de registros adicional realizada sobrescribe las claves SSH preexistentes para el usuario.
- Para la recopilación de registros de soporte con conmutadores NVIDIA, se debe permitir que *user* para la recopilación de registros ejecute `cl-support` el comando sin tener que proporcionar una contraseña. Para permitir este uso, ejecute el comando:

```
echo '<user> ALL = NOPASSWD: /usr/cumulus/bin/cl-support' | sudo EDITOR='tee  
-a' visudo -f /etc/sudoers.d/cumulus
```

Pasos

ONTAP 9.15.1 y versiones posteriores

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.

NOTA: Si responde **y** a la solicitud de especificación del usuario, asegúrese de que el usuario tenga los permisos necesarios como se describe en [Antes de empezar](#) .

```
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
```

```
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>
```



Para CL 5.11.1, cree el usuario **cumulus** y responda **y** al siguiente mensaje: ¿Desea especificar un usuario distinto de admin para la recopilación de registros? {y|n}: **y**

1. **[[paso 2]]**Habilitar la recopilación periódica de registros:

```
system switch ethernet log modify -device <switch-name> -periodic  
-enabled true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -periodic
-enabled true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

cs1: Periodic log collection has been scheduled to run every hour.

```
cluster1::*> system switch ethernet log modify -device cs2 -periodic
-enabled true
```

Do you want to modify the cluster switch log collection configuration? {y|n}: [n] **y**

cs2: Periodic log collection has been scheduled to run every hour.

```
cluster1::*> system switch ethernet log show
```

	Periodic	Periodic
Support		
Switch	Log Enabled	Log State
Log State		
cs1	true	scheduled
never-run		
cs2	true	scheduled
never-run		

2 entries were displayed.

2. Solicitar recogida de registros de soporte:

```
system switch ethernet log collect-support-log -device <switch-name>
```

```
cluster1::*> system switch ethernet log collect-support-log -device
cs1
```

cs1: Waiting for the next Ethernet switch polling cycle to begin support collection.

```
cluster1::*> system switch ethernet log collect-support-log -device
cs2
```

cs2: Waiting for the next Ethernet switch polling cycle to begin support collection.

```
cluster1::*> *system switch ethernet log show
```

	Periodic	Periodic
Support		
Switch	Log Enabled	Log State
Log State		
cs1	false	halted
initiated		
cs2	true	scheduled
initiated		

2 entries were displayed.

3. Para ver todos los detalles de la recogida de registros, incluida la habilitación, el mensaje de estado, la marca de hora y el nombre de archivo anteriores de la recogida periódica, el estado de la solicitud, el mensaje de estado, y la marca de hora y el nombre de archivo anteriores de la recogida de soporte, utilice lo siguiente:

```
system switch ethernet log show -instance
```

```

cluster1::*> system switch ethernet log show -instance

Switch Name: cs1
Periodic Log Enabled: true
Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
Last Periodic Log Timestamp: 3/11/2024 11:02:59
Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
Support Log Requested: false
Support Log Status: Successfully gathered support logs
- see filename for their location.
Last Support Log Timestamp: 3/11/2024 11:14:20
Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

Switch Name: cs2
Periodic Log Enabled: false
Periodic Log Status: Periodic collection has been
halted.
Last Periodic Log Timestamp: 3/11/2024 11:05:18
Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
Support Log Requested: false
Support Log Status: Successfully gathered support logs
- see filename for their location.
Last Support Log Timestamp: 3/11/2024 11:18:54
Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.

```

ONTAP 9.14.1 y anteriores

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.

NOTA: Si responde *y* a la solicitud de especificación del usuario, asegúrese de que el usuario tiene los permisos necesarios como se describe en [Antes de empezar](#).

```
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
```

```
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>
```



Para CL 5.11.1, cree el usuario **cumulus** y responda **y** al siguiente mensaje: ¿Desea especificar un usuario distinto de admin para la recopilación de registros? {y|n}: **y**

1. **[[paso 2]]** Para solicitar la recopilación de registros de soporte y habilitar la recopilación periódica, ejecute el siguiente comando. Esto inicia ambos tipos de recopilación de registros: Los registros detallados `Support` y una recogida de datos por hora `Periodic`.

```
system switch ethernet log modify -device <switch-name> -log-request  
true
```

```
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 la función de recopilación de registros informa de algún estado de error (visible en la salida de `system switch ethernet log show`), consulte ["Solución de problemas de recopilación de registros"](#) para obtener más información.

El futuro

["Configure SNMPv3 \(opcional\)"](#).

Opcional: Configure SNMPv3 para su switch

SNMP se utiliza para supervisar los switches. La monitorización mediante SNMPv3 se configura siguiendo este procedimiento.

El monitor de estado del switch Ethernet (CSHM) utiliza SNMP para supervisar el estado y el rendimiento del clúster y los switches de almacenamiento. De forma predeterminada, SNMPv2c se configura automáticamente a través del archivo de configuración de referencia (RCF). SNMPv3 es más seguro que SNMPv2 porque introduce características de seguridad robustas como la autenticación, el cifrado y la integridad de los mensajes, que protegen contra el acceso no autorizado y garantizan la confidencialidad y la integridad de los datos durante la transmisión.



- SNMPv3 solo es compatible con ONTAP 9.12.1 y versiones posteriores.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 y versiones posteriores solucionan estos dos problemas:
 - "Para la monitorización del estado de ONTAP de los conmutadores Cisco, es posible que aún se vea tráfico SNMPv2 después de cambiar a SNMPv3 para la monitorización."
 - "Alertas de ventilador y de alimentación de interruptores falsos positivos cuando se producen fallos de SNMP"

Acerca de esta tarea

Los siguientes comandos se utilizan para configurar un nombre de usuario SNMPv3 en los conmutadores **Broadcom, Cisco y NVIDIA**:

Switches Broadcom

Configure un OPERADOR DE RED DE nombre de usuario SNMPv3 en los conmutadores Broadcom BES-53248.

- Para **sin autenticación**:

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- Para **autenticación MD5/SHA**:

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```

- Para autenticación **MD5/SHA con cifrado AES/DES**:

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-md5|auth-sha] [priv-aes128|priv-des]
```

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP:

```
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 status
```

```
(sw1)(Config)# snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>
```

```
(cs1)(Config)# show snmp user snmp
```

Name	Group Name	Auth Meth	Priv Meth	Remote Engine ID
<username>	network-admin	MD5	AES128	8000113d03d8c497710bee

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
```

```
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
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if 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>

```

4. Después de esperar el período de sondeo de CSHM, verifique que el número de serie esté completo para el conmutador Ethernet.

```

system switch ethernet polling-interval show

```

```

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: 10.228.136.24
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: <username>
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if 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

```

Switches Cisco

Configure un nombre de usuario SNMPv3_USER de SNMPv3 en switches Cisco 9336C-FX2:

- 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:

```
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:

```
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
```

```
(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
```

```
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
```

```
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-C9336C-FX2
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
```

```

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-C9336C-FX2
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::*>

```

NVIDIA - CL 5.4.0

Configure un nombre de usuario SNMPv3 SNMPv3_USER en los conmutadores NVIDIA SN2100 que ejecutan CLI 5.4.0:

- Para **sin autenticación**:

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- Para **autenticación MD5/SHA**:

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Para autenticación **MD5/SHA con cifrado AES/DES**:

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```


El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP:

```
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:

```
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:

```
net show snmp status
```

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          4318
Version 1 and 2c Community String Configured
Version 3 Usernames     Not Configured
-----

cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf      2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf 2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
# Auto-generated config file: do not edit. #
agentaddress udp:@mgmt:161
agentxperms 777 777 snmp snmp
agentxsocket /var/agentx/master
createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
ifmib_max_num_ifaces 500
iquerysecname _snmptrapusernameX
master agentx
monitor -r 60 -o laNames -o laErrorMessage "laTable" laErrorFlag != 0
pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
```

```

pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshml! default
rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syservices 72
-rocommunity cshml! default

```

net add/del commands since the last "net commit"

User	Timestamp	Command
-----	-----	-----
-----	-----	-----
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username
SNMPv3User	auth-md5 <password>	encrypt-aes <password>

```

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          24253
Version 1 and 2c Community String Configured
Version 3 Usernames      Configured    <---- Configured
here
-----

```

```

cumulus@sw1:~$

```

2. Configure el usuario SNMPv3 en el lado ONTAP:

```
security login create -user-or-group-name SNMPv3User -application  
snmp -authentication-method usm -remote-switch-ipaddress  
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-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 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored ?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User

```

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
```

```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

```

NVIDIA - CL 5.11.0

Configure un nombre de usuario SNMPv3 SNMPv3_USER en los conmutadores NVIDIA SN2100 que ejecutan CLI 5.11.0:

- Para **sin autenticación**:

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- Para **autenticación MD5/SHA**:

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Para autenticación **MD5/SHA con cifrado AES/DES**:

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

El siguiente comando configura un nombre de usuario SNMPv3 en el lado ONTAP:

```
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:

```
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:

```
nv show system snmp-server
```

```
cumulus@sw1:~$ nv show system snmp-server
                                applied
-----
[username]                      SNMPv3_USER
[username]                      limiteduser1
[username]                      testuserauth
[username]                      testuserauthaes
[username]                      testusernoauth
trap-link-up
  check-frequency                60
trap-link-down
  check-frequency                60
[listening-address]             all
[readonly-community]            $nvsec$94d69b56e921aec1790844eb53e772bf
state                           enabled
cumulus@sw1:~$
```

2. Configure el usuario SNMPv3 en el lado ONTAP:

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-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 (b8:59:9f:09:7c:22)"  
-instance
```

```

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored ?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User

```

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
```



```

cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

```

Compruebe el estado del interruptor

Información general de la comprobación del estado

Los monitores de estado supervisan proactivamente ciertas condiciones críticas de su clúster y generan alertas si detectan una falla o un riesgo.

Para ver las alertas del monitor de estado del switch Ethernet actualmente elevadas, ejecute el comando:

```
system health alert show -monitor ethernet-switch
```

Para ver las alertas de control de estado del switch Ethernet disponibles, ejecute el comando:

```
system health alert definition show -monitor ethernet-switch
```

Gestionar la supervisión de switches Ethernet

En la mayoría de los casos, los conmutadores Ethernet son descubiertos automáticamente por ONTAP y monitoreados por CSHM. El archivo de configuración de referencia (RCF) aplicado al switch, entre otras cosas, habilita el protocolo de detección de Cisco (CDP) y/o el protocolo de detección de capa de enlace (LLDP). Sin embargo, es posible que necesite agregar manualmente un conmutador que no se detecte o

eliminar un conmutador que ya no esté en uso. También puede detener la supervisión activa mientras mantiene el interruptor en la configuración, como durante el mantenimiento.

Cree una entrada de conmutador para que ONTAP pueda supervisarla

Utilice `system switch ethernet create` el comando para configurar y activar manualmente la supervisión de un switch Ethernet especificado. Esto es útil si ONTAP no agrega el conmutador automáticamente, o si ya eliminó el conmutador y desea volver a agregarlo.

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshml! -model NX3132V -type
cluster-network
```

Un ejemplo típico es agregar un conmutador llamado [DeviceName], con la dirección IP 1.2.3.4, y las credenciales SNMPv2c establecidas en **cshml!**. Utilice `-type storage-network` en lugar de `-type cluster-network` si va a configurar un switch de almacenamiento.

Desactive la supervisión sin eliminar el conmutador

Si desea pausar o detener la supervisión de un determinado conmutador, pero aún así conservarlo para una supervisión futura, modifique su `is-monitoring-enabled-admin` parámetro en lugar de eliminarlo.

Por ejemplo:

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled
-admin false
```

Esto le permite conservar los detalles del switch y la configuración sin generar nuevas alertas o nuevas detecciones.

Retire un interruptor que ya no necesite

Se utiliza `system switch ethernet delete` para eliminar un interruptor que se ha desconectado o que ya no es necesario:

```
system switch ethernet delete -device DeviceName
```

De manera predeterminada, este comando solo se ejecuta correctamente si ONTAP no detecta actualmente el switch a través de CDP o LLDP. Para quitar un conmutador detectado, utilice el `-force` parámetro:

```
system switch ethernet delete -device DeviceName -force
```

Cuando `-force` se utiliza, el interruptor puede volver a añadirse automáticamente si ONTAP lo detecta de nuevo.

Compruebe la supervisión de los conmutadores Ethernet

El monitor de estado del switch Ethernet (CSHM) intenta monitorizar automáticamente los conmutadores que detecta; sin embargo, es posible que la supervisión no se realice automáticamente si los conmutadores no están configurados correctamente. Debe verificar que el monitor de estado esté correctamente configurado para supervisar los switches.

Confirmar la supervisión de los switches Ethernet conectados

Para confirmar que se están supervisando los conmutadores Ethernet conectados, ejecute:

```
system switch ethernet show
```

Si la `Model` columna muestra **OTHER** o el `IS Monitored` campo muestra **false**, ONTAP no puede monitorear el conmutador. Un valor de **OTHER** normalmente indica que ONTAP no admite ese cambio para el monitoreo de salud.

El `IS Monitored` campo se establece en **false** por el motivo especificado en el `Reason` campo.



Si un conmutador no aparece en la salida del comando, es probable que ONTAP no lo haya descubierto. Confirme que el interruptor esté cableado correctamente. Si es necesario, puede agregar el conmutador manualmente. Consulte ["Gestionar la supervisión de switches Ethernet"](#) Para más detalles.

Confirme que el firmware y las versiones de RCF están actualizadas

Asegúrese de que el switch esté ejecutando el firmware más reciente compatible y de que se haya aplicado un archivo de configuración de referencia compatible (RCF). Más información está disponible en el ["Página de descargas de soporte de NetApp"](#).

De forma predeterminada, el monitor de estado utiliza SNMPv2c con la cadena comunitaria **cshn1!** para el monitoreo, pero también se puede configurar SNMPv3.

Si necesita cambiar la cadena de comunidad SNMPv2c predeterminada, asegúrese de que la cadena de comunidad SNMPv2c deseada se haya configurado en el switch.

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c  
-community-or-username newCommunity!
```



Consulte ["Opcional: Configure SNMPv3"](#) para obtener más información sobre la configuración de SNMPv3 para su uso.

Confirme la conexión de red de gestión

Compruebe que el puerto de gestión del switch está conectado a la red de gestión.

Se requiere una conexión de puerto de gestión correcta para que ONTAP ejecute consultas SNMP y recopile

registros.

Solucionar problemas de alertas

Las alertas se generan si se detecta un fallo, un riesgo o una condición crítica en un switch Ethernet de su clúster.

Si hay alertas activas, el estado del sistema informa del estado Degradado del clúster. Las alertas emitidas incluyen la información que necesita para responder al estado del sistema degradado.

Para ver las alertas de control de estado del switch Ethernet disponibles, ejecute el comando: `system health alert definition show -monitor ethernet-switch`

Consulte el artículo de la base de conocimientos ["Guía de resolución de alertas del monitor de estado del switch"](#) para obtener información detallada sobre la resolución avanzada de las alertas.

Recopilación de registros

Descripción general de la recopilación de registros

Al configurar la recogida de registros, es posible habilitar una recogida horaria de datos periódicos recogidos por AutoSupport, y solicitar registros de soporte detallados.

Consulte ["Configure la recopilación de registros"](#) para obtener más información.

Solución de problemas de recopilación de registros

Si encuentra alguno de los siguientes estados de error indicados por la función de recopilación de registros (visibles en la salida del `system switch ethernet log show` comando), intente 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.
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.



Si los detalles de la resolución no funcionan, póngase en contacto con el soporte de NetApp.

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"](#)

Anuncios de fin de venta y fin de vida útil

- ["Anuncio de fin de venta y fin de vida útil de Nexus 3232C de Cisco"](#)
- ["Anuncio de fin de venta y fin de vida útil de Cisco Nexus 31108PC-V, 31108TC-V y Nexus 3132Q-V."](#)
- ["Anuncio de fin de venta y fin de vida útil de Cisco N9K-C93120TX, N9K-C92300YC"](#)
- ["Anuncio de fin de venta y fin de vida útil de los switches de la serie Nexus 5500 de Cisco"](#)
- ["Fin de la disponibilidad: SKU de interconexión de clúster NetApp CN1610"](#)

Cisco Nexus 3232C

Manos a la obra

Flujo de trabajo de instalación y configuración para conmutadores 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.

Siga estos pasos de flujo de trabajo para instalar y configurar su conmutador Cisco Nexus 3232C.

1

["Requisitos de configuración"](#)

Revise los requisitos de configuración para el conmutador de clúster 3232C.

2

["Documentación requerida"](#)

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores 3232C y el clúster ONTAP .

3

["Requisitos de Smart Call Home"](#)

Revise los requisitos de la función Cisco Smart Call Home, que se utiliza para monitorear los componentes de hardware y software de su red.



"Instale el hardware"

Instale el hardware del interruptor.



"Configurar el software"

Configurar el software del conmutador.

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.

¿Qué sigue?

["Documentación requerida"](#) .

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.

Título del documento	Descripción
<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.
<i>Notas de la versión de Cisco Nexus serie 3000 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 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 de "ONTAP 9" .

Nombre	Descripción
<i>Específicos del controlador 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.

Nombre	Descripción
"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 Smart Call Home, debe configurar un conmutador de red de clúster para comunicarse mediante correo electrónico con el sistema Smart Call Home. Además, puede configurar opcionalmente su conmutador de red de clúster para aprovechar la función de soporte Smart Call Home integrada de Cisco.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Antes de poder utilizar Smart Call Home, tenga en cuenta los siguientes requisitos:

- Debe haber un servidor de correo electrónico.
- 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

Flujo de trabajo de instalación de hardware para conmutadores Cisco Nexus 3232C

Para instalar y configurar el hardware de un conmutador de clúster 3232C, siga estos pasos:

1 "Complete la hoja de trabajo 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.

2 "Instale el interruptor"

Instale el interruptor 3232C.

3 "Instale el interruptor en un armario NetApp"

Instale el conmutador 3232C y el panel de paso en un gabinete NetApp según sea necesario.

4 "Revisar el cableado y la configuración"

Revise el soporte para puertos Ethernet NVIDIA .

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

Switch de clúster a		Switch del clúster B	
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
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

Switch de clúster a		Switch del clúster B	
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	
3		3	
4		4	
5		5	
6		6	

Switch de clúster a		Switch del clúster B	
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	
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

¿Qué sigue?

["Instale el interruptor"](#) .

Instalar el conmutador de clúster 3232C

Siga este procedimiento para configurar el switch Cisco Nexus 3232C.

Antes de empezar

Asegúrese de tener lo siguiente:

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones 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.
- Las licencias aplicables, la información de configuración y red, y los cables.
- Terminado ["hojas de datos para el cableado"](#) .
- Los RCF de red de gestión y red de clúster de NetApp aplicables descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#). 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.
- ["Documentación necesaria sobre el switch y ONTAP"](#) .

Pasos

1. Monte en rack la red del clúster y los switches de red de gestión y las controladoras.

Si está instalando...	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.

El futuro

Opcionalmente, puedes ["Instalar un conmutador Cisco Nexus 3223C en un gabinete NetApp"](#) . De lo contrario, vaya a ["Revisar el cableado y la configuración"](#) .

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.

Antes de empezar

- 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

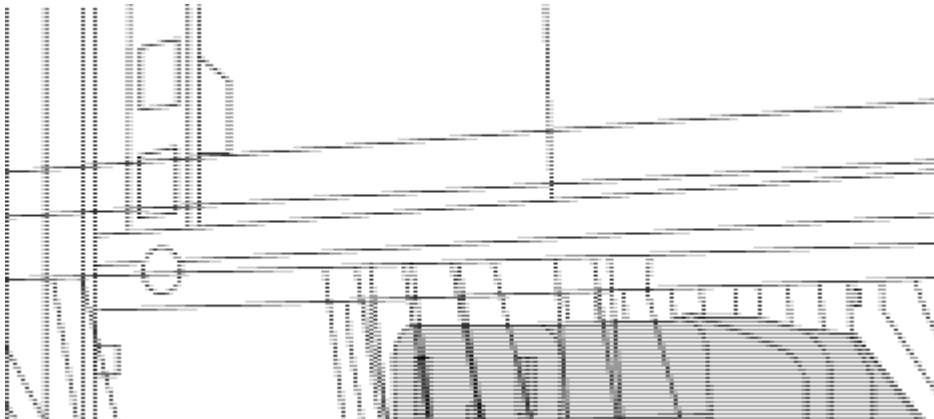
1. Instale el panel de borrado de paso en el armario de NetApp.

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.

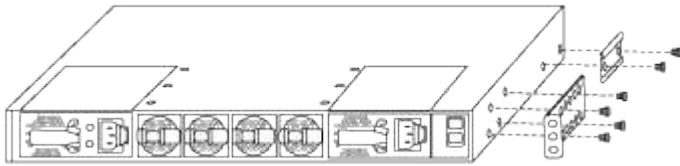
En este procedimiento, el panel de limpieza se instalará en U40.
 - ii. Instale dos tuercas de abrazadera a cada lado en los orificios cuadrados adecuados para los rieles delanteros del armario.
 - iii. Centre el panel verticalmente para evitar intrusiones en el espacio adyacente del bastidor y, a continuación, 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.



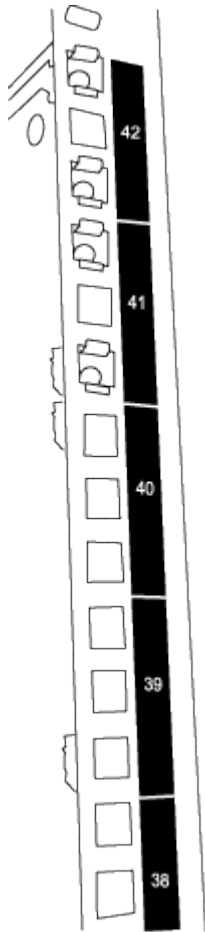
(1) conector hembra del cable puente.

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.

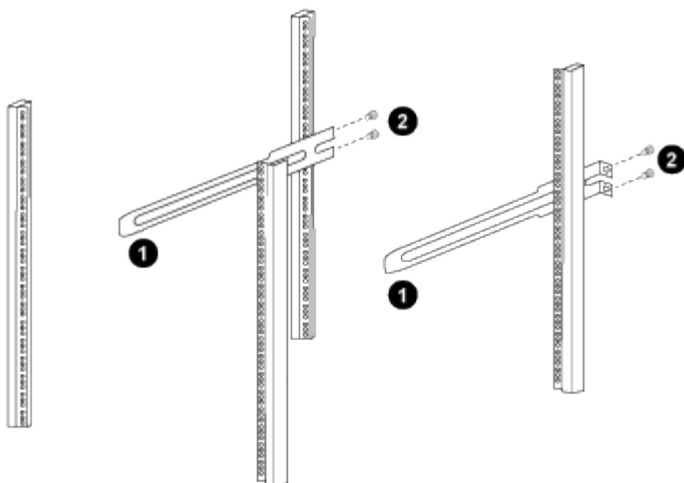


- b. Repita el paso 2a con el otro soporte de montaje en bastidor delantero en el otro lado del interruptor.
 - c. Instale el soporte de montaje en bastidor trasero en el chasis del interruptor.
 - d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del interruptor.
2. 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 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 los rieles deslizantes a los postes del armario.

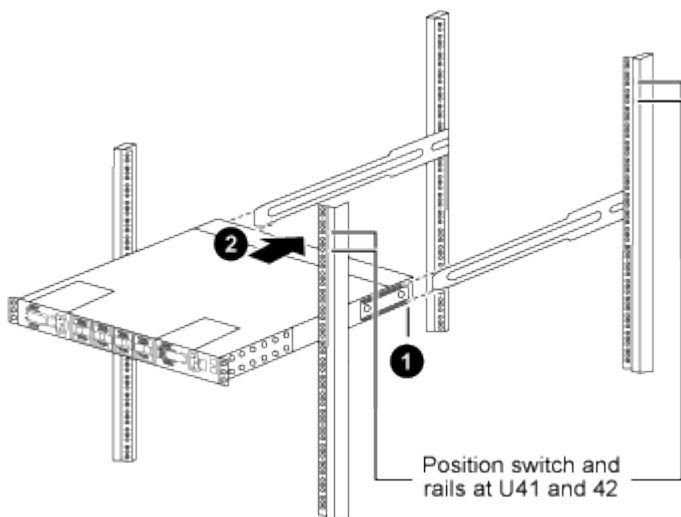
- a. Repita el paso 4a para el poste trasero derecho.
- b. Repita los pasos 4a y 4b en las ubicaciones RU41 del armario.

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.

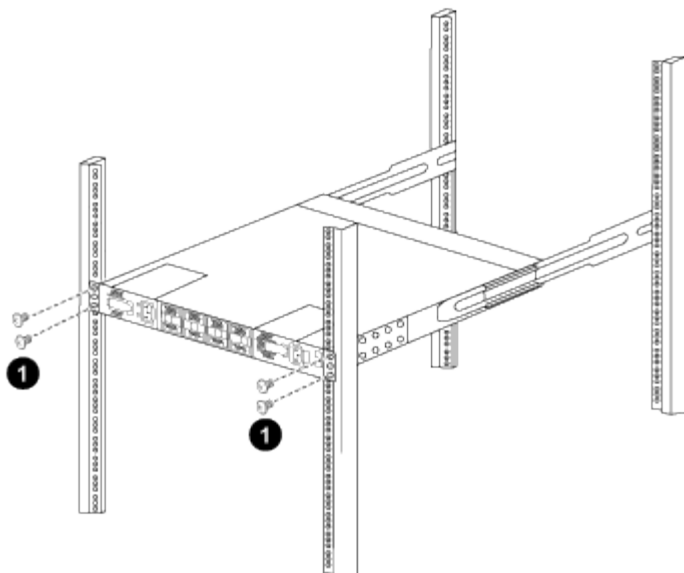
- a. Coloque la parte posterior del interruptor en RU41.



(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

Flujo de trabajo de instalación de software para conmutadores de clúster Cisco Nexus 3232C

Para instalar y configurar el software de un conmutador Cisco Nexus 3232C e instalar o actualizar el archivo de configuración de referencia (RCF), siga estos pasos:

1

"Configure el switch"

Configurar el conmutador de clúster 3232C.

2

"Prepárese para instalar el software NX-OS y RCF"

El software Cisco NX-OS y los archivos de configuración de referencia (RCF) deben estar instalados en los conmutadores de clúster Cisco 3232C.

3

"Instale o actualice el software NX-OS"

Descargue e instale o actualice el software NX-OS en el conmutador de clúster Cisco 3232C.

4

"Instale el RCF"

Instale el RCF después de configurar el conmutador Cisco 3232C por primera vez.

5

"Compruebe la configuración de SSH"

Verifique que SSH esté habilitado en los conmutadores para usar el Monitor de estado del conmutador Ethernet (CSHM) y las funciones de recopilación de registros.

6

"Restablecer el interruptor a los valores predeterminados de fábrica"

Borre la configuración del interruptor del grupo 3232C.

Configure el switch del clúster 3232C

Siga este procedimiento para configurar el switch Cisco Nexus 3232C.

Antes de empezar

- 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
¿Habilitar el servicio telnet? (sí/no)	Responda con no . El valor predeterminado es no

Prompt	Respuesta
¿Servicio SSH habilitado? (sí/no)	Responda con sí. El valor predeterminado es yes.  Se recomienda SSH cuando se utiliza Ethernet Switch Health Monitor (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.
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)	Responda con sí para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.  Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador.

5. 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 el software NX-OS

Puede utilizar este procedimiento para instalar el software NX-OS en el switch de clúster Nexus 3232C.

Revise los requisitos

Antes de empezar

- 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. 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::*>
```

4. Compruebe el estado administrativo y operativo de cada puerto del clúster.

a. Compruebe que todos los puertos del clúster están **up** con un 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                                     Type                Address
Model                                     -----
-----
cs1                                       cluster-network     10.233.205.90      N3K-
C3232C
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                       cluster-network     10.233.205.91      N3K-
C3232C
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

6. 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.
```

7. 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 FOCXXXXXXGD

  Device name: cs2
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 36 second(s)

Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(3)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

8. Instale la imagen NX-OS.

La instalación del archivo de imagen 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#
```

9. 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 08.37
  NXOS: version 9.3(4)
  BIOS compile time: 01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 06:28:31]

Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGS

  Device name: rtpnpi-mcc01-8200-ms-A1
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)

Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
Reason: Reset due to upgrade
```

```
System version: 9.3(3)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

10. Actualice la imagen 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#

- Si va a actualizar a NX-OS versión 9,3(11), debe actualizar la imagen EPLD golden y reiniciar el conmutador una vez más. De lo contrario, vaya al paso 12.

Consulte "[Notas de la versión de actualización de EPLD, versión 9,3\(11\)](#)" para obtener más información.

Muestra el ejemplo

```
cs2# install epld bootflash:n9000-epld.9.3.11.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module          Type          Upgradable      Impact          Reason
-----
-----
          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#
```

12. 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

13. 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 -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
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 Model	Type	Address	
cs1	cluster-network	10.233.205.90	N3K-
C3232C			
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	N3K-

```

C3232C
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

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.

```

14. 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::*>

```

15. Repita los pasos 6 a 14 en el interruptor CS1.

16. Habilite la reversión automática en las LIF del clúster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

17. 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 LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

El futuro

["Instale el archivo de configuración RCF".](#)

Instale o actualice el RCF

Instale o actualice la descripción general del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar los conmutadores Nexus 3232C por primera vez. Actualiza tu versión RCF cuando tienes

una versión existente del archivo RCF instalado en tu conmutador.

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) para obtener más información al instalar o actualizar su RCF.

Configuraciones de RCF disponibles

En la siguiente tabla se describen los CFR disponibles para diferentes configuraciones. Seleccione el RCF aplicable a su configuración.

Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

Nombre de RCF	Descripción
2-Cluster-HA-Breakout	Admite dos clústeres ONTAP con al menos ocho nodos, incluidos los nodos que utilizan puertos compartidos Cluster+HA.
4-Cluster-HA-Breakout	Admite cuatro clústeres ONTAP con al menos cuatro nodos, incluidos los nodos que utilizan puertos compartidos Cluster+HA.
1-Cluster-HA	Todos los puertos están configurados para 40/100GbE. Admite el tráfico de clúster/alta disponibilidad compartido en los puertos. Necesario para los sistemas AFF A320, AFF A250 y FAS500f. Además, todos los puertos se pueden utilizar como puertos de clúster dedicados.
1-Cluster-HA-Breakout	Los puertos se configuran para 4 puertos de separación de 10 GbE, 4 GbE (RCF 1,6+ en switches 100GbE) y 40/100GbE. Admite el tráfico compartido de clúster/alta disponibilidad en los puertos para los nodos que utilizan puertos de clúster/alta disponibilidad compartidos: Sistemas AFF A320, AFF A250 y FAS500f. Además, todos los puertos se pueden utilizar como puertos de clúster dedicados.
Cluster-HA-Storage	Los puertos se configuran para 40/100GbE para clúster+HA, 4 puertos separados de 10 GbE para clúster y 4 GbE para clúster+HA, y 100GbE para cada par de alta disponibilidad de almacenamiento.
Clúster	Dos variantes de RCF con diferentes asignaciones de 4 puertos 10 GbE (breakout) y de puertos 40/100GbE. Todos los nodos FAS/AFF son compatibles, excepto para los sistemas AFF A320, AFF A250 y FAS500f.
Reducida	Todos los puertos se configuran para conexiones de almacenamiento NVMe de 100GbE Gb.

Documentación sugerida

- ["Switches Ethernet de Cisco \(NSS\)"](#)

Consulte la tabla de compatibilidad de switches para conocer las versiones de ONTAP y RCF compatibles en el sitio de soporte de NetApp. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis del comando en el RCF y la sintaxis encontrada en versiones específicas de NX-OS.

- ["Switches Cisco Nexus serie 3000"](#)

Consulte las guías de software y actualización correspondientes disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación del conmutador Cisco.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos interruptores Cisco son **CS1** y **CS2**.
- Los nombres de los nodos son **cluster1-01**, **cluster1-02**, **cluster1-03** y **cluster1-04**.
- Los nombres de LIF de los clústeres son **cluster1-01_clus1**, **cluster1-04_clus2**, **cluster1-03_clus2**, **cluster1-03_clus1**, **cluster1-02_clus2**, **cluster1-02_clus1**, **cluster1-01_clus1** y **cluster1-04_clus1**.
- La `cluster1::*>` prompt indica el nombre del clúster.

En los ejemplos de este procedimiento se utilizan cuatro nodos. Estos nodos utilizan dos puertos de interconexión de clúster 10GbE **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.

Para obtener detalles de las configuraciones RCF disponibles, consulte ["Flujo de trabajo de instalación del software"](#).

Comandos utilizados

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 futuro

Después de haber revisado el procedimiento de instalación o actualización de RCF, ["instalar el RCF"](#) o ["Mejora tu RCF"](#) según sea necesario.

Instalación del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar los conmutadores Nexus 3232C por primera vez.

Antes de empezar

Compruebe las siguientes instalaciones y conexiones:

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El RCF actual.
- Una conexión de consola al conmutador, necesaria para instalar el RCF.

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.

No se necesita ningún enlace entre conmutadores (ISL) operativo durante este procedimiento. Esto es así por

diseño porque los cambios de versión de RCF pueden afectar la conectividad de ISL temporalmente. Para habilitar operaciones de clúster sin interrupciones, el siguiente procedimiento migra todos los LIF del clúster al conmutador del socio operativo mientras se realizan los pasos en el conmutador de destino.

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.

Paso 1: Instale el RCF en los interruptores

1. Inicie sesión para cambiar cs2 usando SSH o mediante una consola serial.
2. Copie el RCF al bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) .

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)...
```

3. Aplique el RCF descargado anteriormente al flash de inicio.

Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 3000"](#) .

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
```



Asegúrese de leer detenidamente las secciones **Notas de instalación**, **Notas importantes** y **banner** de su RCF. Debe leer y seguir estas instrucciones para garantizar la configuración y el funcionamiento adecuados del conmutador.

4. 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.

5. 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.

6. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.

7. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.



Asegúrese de configurar lo siguiente: * Nombre de usuario y contraseña * Dirección IP de administración * Puerta de enlace predeterminada * Nombre del conmutador

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

8. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>  
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region qos 256" >>  
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) Para más detalles.

9. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

```
show file bootflash:write_erase.cfg
```

10. Emitir el `write erase` Comando para borrar la configuración guardada actual:

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] **y**

11. Copie la configuración básica guardada anteriormente en la configuración de inicio.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

12. Interruptor de reinicio cs2:

```
cs2# reload
```

This command will reboot the system. (y/n)? [n] **y**

13. Repita los pasos 1 a 12 en el interruptor cs1.
14. Conecte los puertos de clúster de todos los nodos del clúster de ONTAP a los switches CS1 y CS2.

Paso 2: Verifique las conexiones del conmutador

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
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 -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 algún LIFS del clúster no ha regresado a sus puertos de origen, revuértalo manualmente:

```
network interface revert -vserver <vserver_name> -lif <lif_name>
```

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
4 entries were displayed.
cluster1::*>
```

Paso 3: Configure su clúster ONTAP

NetApp recomienda usar System Manager para configurar clústeres nuevos.

System Manager proporciona un flujo de trabajo simple y fácil para la configuración y el establecimiento de un clúster, incluida la asignación de una dirección IP de administración de nodo, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento de almacenamiento inicial.

Referirse a ["Configure ONTAP en un nuevo clúster con System Manager"](#) para obtener instrucciones de configuración.

El futuro

Después de haber instalado el RCF, ["verificar la configuración de SSH"](#).

Actualice su archivo de configuración de referencia (RCF)

Actualice la versión de RCF cuando tenga instalada una versión existente del archivo RCF en los conmutadores operativos.

Antes de empezar

Asegúrese de tener lo siguiente:

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El RCF actual.
- Si está actualizando la versión de RCF, necesita una configuración de inicio en el RCF que refleje las imágenes de inicio deseadas.

Si necesita cambiar la configuración 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.



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.



Antes de instalar una nueva versión de software del conmutador y RCF, debe borrar los ajustes del conmutador y realizar la configuración básica. Debe estar conectado al switch mediante la consola serie o haber conservado la información básica de configuración antes de borrar la configuración del switch.

Paso 1: Prepárese para la actualización

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
```

Speed (Mbps)

```

Health   Health
Port     IPspace   Broadcast Domain Link MTU   Admin/Oper
Status   Status
-----
e0a      Cluster   Cluster           up    9000   auto/10000
healthy  false
e0b      Cluster   Cluster           up    9000   auto/10000
healthy  false
cluster1::*>

```

b. 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
          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
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                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.92
NX3232C
    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
NX3232C
    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
```

Paso 2: Configurar puertos

1. En el switch de clúster cs2, apague los puertos conectados a los puertos del clúster de los nodos.


```
cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit
```



Asegúrese de cerrar * todos * puertos de clúster conectados para evitar cualquier problema de conexión de red. Consulte el artículo de la base de conocimientos ["Nodo fuera de quórum al migrar LIF de clúster durante la actualización del sistema operativo del switch"](#) para obtener más información.

2. Verifique que los puertos del clúster hayan conmutado por error a los puertos alojados en el conmutador de clúster cs1. Esto podría 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::*>				

3. 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::*>
```

4. 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
```

5. Registre cualquier adición personalizada entre la actual `running-config` y el archivo RCF en uso (como una configuración SNMP para su organización).
6. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.



Asegúrese de configurar lo siguiente: * Nombre de usuario y contraseña * Dirección IP de administración * Puerta de enlace predeterminada * Nombre del conmutador

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

7. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region qos 256" >>
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) Para más detalles.

8. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

```
show file bootflash:write_erase.cfg
```

9. Emitir el `write erase` Comando para borrar la configuración guardada actual:

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] **y**

10. Copie la configuración básica guardada anteriormente en la configuración de inicio.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

11. Reiniciar el switch cs2:

```
cs2# reload
```

This command will reboot the system. (y/n)? [n] **y**

12. Cuando se pueda volver a acceder a la dirección IP de administración, inicie sesión en el switch a través de SSH.

Es posible que necesite actualizar las entradas del archivo host relacionadas con las claves SSH.

13. Copie el RCF al bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos 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)...
```

14. 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
```



Asegúrese de leer detenidamente las secciones **Notas de instalación**, **Notas importantes** y **banner** de su RCF. Debe leer y seguir estas instrucciones para garantizar la configuración y el funcionamiento adecuados del conmutador.

15. 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.

16. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.
17. 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
```

18. 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
```

19. 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
```

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.

```

- 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.
```



Es posible que observe la siguiente salida en la consola del conmutador cs1 según la versión de 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. Se restableció la consistencia del puerto. 17 nov 2020 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_PEER: Bloqueo del canal de puerto 1 en VLAN0001. VLAN de pares inconsistente. 17 nov 2020 16:07:23 cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_LOCAL: Bloqueando el canal de puerto 1 en VLAN0092. VLAN local inconsistente.



Los nodos del clúster pueden tardar hasta 5 minutos en informar en buen estado.

20. 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
```

21. 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::*>				

22. 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::*>
```

23. Repita los pasos 4 a 19 en el interruptor cs1.
24. Habilite la reversión automática en las LIF del clúster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert true
```

Paso 3: Compruebe la configuración de la red del clúster y el estado del clúster

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
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 -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
```

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
4 entries were displayed.
cluster1::*>
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puedes utilizar el `network interface check cluster-connectivity` Comando para iniciar una verificación de accesibilidad para la conectividad del clúster y luego mostrar los detalles:

```
network interface check cluster-connectivity start y network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

cluster1-01			
	3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02_clus1
none			
	3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-02_clus2
none			
.			
.			
cluster1-02			
	3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-01_clus1
none			
	3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-01_clus2
none			
.			
.			
cluster1-03			
.			
.			
.			
.			
cluster1-04			
.			
.			
.			
.			

Todos los lanzamientos de ONTAP

Para todas las versiones de ONTAP , también puedes usar el

cluster ping-cluster -node <name> Comando para comprobar la conectividad:
cluster ping-cluster -node <name>

```
cluster1::~*> cluster ping-cluster -node local
Host is cluster1-03
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)
```

El futuro

Después de haber actualizado su RCF, ["verificar la configuración de SSH"](#) .

Compruebe su configuración SSH

Si utiliza la supervisión de estado del switch Ethernet (CSHM) y las funciones de recogida de registros, compruebe que las claves SSH y SSH estén habilitadas en los switches de clústeres.

Pasos

1. Compruebe que SSH está habilitado:

```
(switch) show ssh server  
ssh version 2 is enabled
```

2. Compruebe que las claves SSH estén habilitadas:

```
show ssh key
```

Muestra el ejemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yIPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDsrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(switch)# show feature | include scpServer
scpServer          1          enabled
(switch)# show feature | include ssh
sshServer          1          enabled
(switch)#
```



Al habilitar FIPS, debe cambiar el bitcount a 256 en el conmutador mediante el comando `ssh key ecdsa 256 force`. Consulte ["Configurar la seguridad de red con FIPS"](#) para obtener más información.

El futuro

["Configure la supervisión de estado del switch"](#).

Restablecer el interruptor del clúster 3232C a los valores predeterminados de fábrica

Para restablecer el interruptor del clúster 3232C a los valores predeterminados de fábrica, debe borrar la configuración del interruptor 3232C.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Borrar la configuración existente:

```
write erase
```

```
(cs2)# write erase
```

```
Warning: This command will erase the startup-configuration.  
Do you wish to proceed anyway? (y/n) [n] y
```

2. Recargue el software del conmutador:

```
reload
```

```
(cs2)# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

El sistema se reinicia y entra en el asistente de configuración. Durante el arranque, si recibe el mensaje “¿Desea cancelar el aprovisionamiento automático y continuar con la configuración normal?” (sí/no)[n]”, debe responder **sí** para continuar.

Migrar switches

Migración de switches de CN1610 GbE

Migre desde switches CN1610 al flujo de trabajo de switches Nexus 3232C

Siga estos pasos del flujo de trabajo para migrar sus switches CN1610 a los switches Nexus 3232C de Cisco.

1

"Requisitos de migración"

Revise la información del switch de ejemplo para el proceso de migración.

2

"Prepare la migración"

Prepare los switches CN1610 para la migración a los switches Nexus 3232C.

3

"Reemplace el interruptor del grupo de instrumentos CL2"

Sustituya el switch de clúster CL2 por el nuevo switch Nexus 3232C C2.

4

"Reemplace el interruptor del grupo de instrumentos CL1"

Sustituya el switch de clúster CL1 por el nuevo switch Nexus 3232C C1.

5

"Completa la migración"

Complete la migración a los nuevos switches Nexus 3232C.

Requisitos de migración

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.



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:

- ["NetApp CN1601 y CN1610"](#)
- ["Switches Ethernet de Cisco"](#)
- ["Hardware Universe"](#)

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

Debes haber descargado los archivos de configuración de referencia (RCF) aplicables. La cantidad de puertos de 10 GbE y 40/100 GbE se define en los RCF disponibles en ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) .

Las versiones de ONTAP y NX-OS compatibles con este procedimiento se enumeran en ["Switches Ethernet de Cisco"](#) .

Las versiones de ONTAP y FASTPATH compatibles con este procedimiento se enumeran en ["Switches CN1601 y CN1610 de NetApp"](#) .

Acerca de los ejemplos utilizados

En los ejemplos del procedimiento de migración se 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 GbE: **E4A** y **E4E**.

El ["Hardware Universe"](#) tiene información sobre los cables de fibra de clúster para 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 CN1610 interruptores que se van a sustituir son **CL1** y **CL2**.
- Los switches Nexus 3232C para reemplazar los interruptores CN1610 son **C1** y **C2**.
- **n1_clus1** es la primera interfaz lógica de clúster (LIF) que está conectada al conmutador de clúster 1 (CL1 o C1) para el nodo **n1**.
- **n1_clus2** es el primer LIF de clúster que está conectado al conmutador de clúster 2 (CL2 o C2) para el nodo **n1**.
- **n1_clus3** es el segundo LIF que está conectado al conmutador de cluster 2 (CL2 o C2) para el nodo **n1**.
- **n1_clus4** es el segundo LIF que está conectado al conmutador de cluster 1 (CL1 o C1) para el nodo **n1**.
- La cantidad de puertos de 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#) .

El futuro

["Prepare la migración"](#).

Siga estos pasos para preparar la migración del switch CN1610 a un switch Cisco Nexus 3232C.

Pasos

- 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.

- 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.

- Determinar el estado administrativo u operativo de cada interfaz de clúster.

- 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. Ver ["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. Seleccione **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 apropiada del software de imágenes 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
false     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       e0a
false     n2_clus3    up/up      10.10.0.7/24  n2       e0d
false     n2_clus4    up/up      10.10.0.8/24  n2       e0d
true

8 entries were displayed.
```

El futuro

"[Reemplace el interruptor CN1610 CL2 por el interruptor 3232C C2](#)".

Reemplace el interruptor CN1610 CL2 por el interruptor 3232C C2

Siga estos pasos para sustituir el switch CN1610 (CL2) por un switch Nexus 3232C (C2).

Pasos

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

			Source	Destination
Packet				
Node	Date		LIF	LIF
Loss				
-----	-----	-----	-----	-----

n1				
	3/5/2022 19:21:18 -06:00		n1_clus2	n2-clus1
none				
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2
none				
n2				
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1
none				
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2
none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

1. Apague los puertos ISL 13 a 16 en el conmutador CN1610 activo CL1 con el comando apropiado.

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) #
```

2. 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
```

3. 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.

4. 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.

5. 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) #
```

6. 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) #
```

7. 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		

8. 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)
```

9. 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
```

10. 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
```

11. 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
true

8 entries were displayed.
```

12. 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.

13. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

			Source	Destination
Packet				
Node	Date		LIF	LIF
Loss				
-----	-----	-----	-----	-----

n1				
	3/5/2022 19:21:18 -06:00		n1_clus2	n2-clus1
none				
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2
none				
n2				
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1
none				
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2
none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

1. Migre las LIF asociadas al primer switch de CN1610 CL1:

```

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
```

El futuro

"Reemplace el interruptor CN1610 CL1 por el interruptor 3232C C1".

Reemplace el interruptor CN1610 CL1 por el interruptor 3232C C1

Siga estos pasos para sustituir el switch CN1610 (CL1) por un switch Nexus 3232C (C1).

Pasos

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.
```

El futuro

"Completa la migración".

Complete la migración de CN1610 switches a 3232C switches

Complete los siguientes pasos para finalizar la migración de switches CN1610 a los switches Nexus 3232C.

Pasos

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

			Source	Destination
Packet				
Node	Date		LIF	LIF
Loss				
-----	-----	-----	-----	-----

n1				
	3/5/2022 19:21:18 -06:00		n1_clus2	n2-clus1
none				
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2
none				
n2				
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1
none				
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2
none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

1. Ampliar el clúster agregando nodos a los switches de clúster Nexus 3232C.
2. 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.

```

3. 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

```

4. 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.

5. Si ha suprimido la creación automática de casos, rehabilitarla invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

El futuro

["Configure la supervisión de estado del switch".](#)

Migración de switch Nexus 5596

Migre de switches Nexus 5596 al flujo de trabajo de switches Nexus 3232C

Siga estos pasos del flujo de trabajo para migrar sus switches Cisco Nexus 5596 a switches Cisco Nexus 3232C.

1**"Requisitos de migración"**

Revise la información del switch de ejemplo para el proceso de migración.

2**"Prepare la migración"**

Prepare los switches Nexus 5596 para la migración a los switches Nexus 3232C.

3**"Configure los puertos"**

Configure sus puertos para la migración a los nuevos switches Nexus 3232C.

4**"Completa la migración"**

Complete la migración a los nuevos switches Nexus 3232C.

Requisitos de migración

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.



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:

- ["Switches Ethernet de Cisco"](#)
- ["Hardware Universe"](#)

Requisitos de Cisco Nexus 5596

Los switches de clúster utilizan los siguientes puertos para las conexiones a los nodos:

- Nexus 5596: Puertos E1/1-40 (10 GbE)
- Nexus 3232C: Puertos E1/1-30 (10/40/100 GbE)

Los switches de clúster utilizan los siguientes puertos de enlace entre switches (ISL):

- Nexus 5596: Puertos E1/41-48 (10 GbE)
- Nexus 3232C: Puertos E1/31-32 (40/100 GbE)

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 de ONTAP y NX-OS compatibles con este procedimiento se encuentran en ["Switches Ethernet de Cisco"](#).

Acerca de los ejemplos utilizados

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 switches Nexus 5596 a sustituir son **CL1** y **CL2**.
- Los switches Nexus 3232C para reemplazar los switches Nexus 5596 son **C1** y **C2**.
- **n1_clus1** es la primera interfaz lógica de clúster (LIF) conectada al conmutador de clúster 1 (CL1 o C1) para el nodo **n1**.

- **n1_clus2** es el primer LIF de clúster conectado al conmutador de clúster 2 (CL2 o C2) para el nodo **n1**.
- **n1_clus3** es el segundo LIF conectado al conmutador de cluster 2 (CL2 o C2) para el nodo **n1**.
- **n1_clus4** es el segundo LIF conectado al conmutador de cluster 1 (CL1 o C1) para el nodo **n1**.
- La cantidad de puertos de 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en el sitio web. "[Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®](#)".
- 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**.

En "[Hardware Universe](#)" la se muestran los puertos de clúster reales de las plataformas.

Escenarios cubiertos

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.

El futuro

"[Prepare la migración](#)".

Prepárese para la migración desde switches Nexus 5596 a switches Nexus 3232C

Siga estos pasos para preparar los switches Cisco Nexus 5596 para la migración a los switches Cisco Nexus 3232C.

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
```

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
```

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. 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. Seleccione **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 de descarga *ONTAP 8.x o posterior Archivos de configuración de referencia de switches de red de administración y clúster* y, a continuación, seleccione 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.
```

El futuro

["Configure los puertos"](#).

Configure sus puertos para la migración de los switches Nexus 5596 a los switches Nexus 3232C

Siga estos pasos para configurar los puertos para la migración desde los switches Nexus 5596 a los nuevos switches Nexus 3232C.

Pasos

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet			Source	Destination
Node	Date		LIF	LIF
Loss				

n1				
	3/5/2022 19:21:18 -06:00		n1_clus2	n2-clus1
none				
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2
none				
n2				
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1
none				
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2
none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

1. Apague los ISLs 41 a 48 en CL1, el switch Nexus 5596 activo, utilizando el comando Cisco `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 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) #
```

2. 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
```

3. 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.

4. 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.

5. 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

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)#
```

6. 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)
```

7. Compruebe que las interfaces eth1/45-48 ya tienen "modo de grupo de canal 1 activo" en su configuración de ejecución.

8. 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
```

9. 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
```

10. 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.
```

11. 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
```

						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	-
-							

```
8 entries were displayed.
```

12. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

			Source	Destination
Packet				
Node	Date		LIF	LIF
Loss				
-----	-----	-----	-----	-----

n1				
	3/5/2022 19:21:18 -06:00		n1_clus2	n2-clus1
none				
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2
none				
n2				
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1
none				
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2
none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

1. En cada nodo del cluster, migre las interfaces asociadas con el primer switch Nexus 5596, CL1, para ser reemplazado:

```
network interface migrate -vserver vserver-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
```

2. 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
```

	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
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.				
-----	-----	----		

3. 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
```

4. 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#
```

5. 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.

6. 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.

7. 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.
```

8. 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
```

9. 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)
```

10. 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
```

11. 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.
```

12. 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
```

13. 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)
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.
```

14. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

			Source	Destination
Packet				
Node	Date		LIF	LIF
Loss				
-----	-----	-----	-----	-----

n1				
	3/5/2022 19:21:18 -06:00		n1_clus2	n2-clus1
none				
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2
none				
n2				
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1
none				
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2
none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

1. Ampliar el clúster agregando 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
```

	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

12 entries were displayed.

+

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Speed(Mbps) 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.

+

```
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.
```

2. 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
```

El futuro

["Completa la migración"](#).

Complete la migración de 5596 switches a 3232C switches

Complete los siguientes pasos para finalizar la migración de los switches Nexus 5596 a los switches Nexus 3232C.

Pasos

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. 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
```

El futuro

["Configure la supervisión de estado del switch".](#)

Migre desde clústeres de dos nodos sin switch

Migre desde un flujo de trabajo de clústeres sin switches de dos nodos

Siga estos pasos del flujo de trabajo para migrar desde un clúster de dos nodos sin switch a un clúster con switches de clúster Cisco Nexus 3232C.

1

"Requisitos de migración"

Revise la información del switch de ejemplo para el proceso de migración.

2

"Prepare la migración"

Prepare su clúster de dos nodos sin switches para migrarlo a un clúster con switches de dos nodos.

3

"Configure los puertos"

Configure su clúster de dos nodos sin switches para migrarlo a un clúster con switches de dos nodos.

4

"Completa la migración"

Complete la migración a un clúster con switches de dos nodos.

Requisitos de migración

Si tiene un clúster de dos nodos sin switch, puede migrar a un clúster con switches de dos nodos que incluya switches de red de clústeres Nexus 3232C de Cisco. Se trata de un procedimiento no disruptivo.

Antes de empezar

Compruebe las siguientes instalaciones y conexiones:

- 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 módulos ópticos QSFP/QSFP28 compatibles con cables de fibra o cables de conexión directa de cobre QSFP/QSFP28.
 - Los switches de clúster requieren el cableado ISL adecuado:
 - Cables de conexión directa de fibra o cobre 2x 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

Acerca de los ejemplos utilizados

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Switches de cluster Nexus 3232C, **C1** y **C2**.
- Los nodos son **n1** y **n2**.

Los ejemplos de este procedimiento utilizan dos nodos, cada uno usando dos puertos de interconexión de clúster de 40 GbE **E4A** y **E4E**. El "[Hardware Universe](#)" tiene detalles sobre los puertos de clúster en las plataformas.

- **n1_clus1** es la primera interfaz lógica de clúster (LIF) que se conecta al conmutador de clúster **C1** para el nodo **n1**.
- **n1_clus2** es el primer LIF de clúster que se conecta al conmutador de clúster **C2** para el nodo **n1**.
- **n2_clus1** es el primer LIF de clúster que se conecta al conmutador de clúster **C1** para el nodo **n2**.
- **n2_clus2** es el segundo LIF de clúster que se conecta al conmutador de clúster **C2** para el 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.

El futuro

["Prepare la migración"](#).

Prepárese para la migración desde clústeres de dos nodos sin switch a clústeres con switches de dos nodos

Siga estos pasos para preparar su clúster sin switch de dos nodos para migrar a un clúster con switches de dos nodos que incluya switches de red de clústeres Nexus 3232C de Cisco.

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
```

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
      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.
```

- 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. Seleccione **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 de Cisco"](#)

4. Seleccione **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 sobre los comandos de Cisco, consulte la siguiente lista en la ["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 sobre los comandos de Cisco, consulte la siguiente lista en la ["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 sobre los comandos de Cisco, consulte la siguiente lista en la ["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

El futuro

["Configure los puertos"](#).

Configure sus puertos para la migración de un clúster de dos nodos sin switch a un clúster de dos nodos con switches

Siga estos pasos para configurar los puertos para migrar desde un clúster de dos nodos sin switches a un clúster de dos nodos con switches Nexus 3232C.

Pasos

1. 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
```

2. 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.
```

3. 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
```

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

			Source	Destination
Packet				
Node	Date		LIF	LIF
Loss				
-----	-----	-----	-----	-----

n1				
	3/5/2022 19:21:18 -06:00		n1_clus2	n2-clus1
none				
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2
none				
n2				
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1
none				
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2
none				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

1. Desconecte el cable de E4A en el 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.

2. 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.

3. 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
```

4. 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
```

5. 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.
```

6. 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
```

7. 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.
```

8. 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-C3232C
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	n1	e4e	FAS9000

9. 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
```

10. 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
```

11. 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.
```

12. 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.

13. 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.

14. 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
```

15. 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
```

16. 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
```

El futuro

"Completa la migración".

Complete la migración desde un clúster de dos nodos sin switches a un clúster de dos nodos con switches

Complete los siguientes pasos para finalizar la migración del clúster de dos nodos sin switch a un clúster con switches de dos nodos en switches Nexus 3232C.

Pasos

- 1. 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
      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.
```

- 2. Compruebe que todos los puertos de interconexión del clúster se encuentren en la up provincia:

```
network port show -role cluster
```

- 3. 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
```

Node	Local Port	Discovered 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

4. Mostrar switches de cl ster 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.

5. Compruebe que la detección del clúster sin switches ha cambiado la opción de clúster sin switches a deshabilitado:

```
network options switchless-cluster show
```

6. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
n1					
	3/5/2022 19:21:18 -06:00		n1_clus2		n2-clus1
none					
	3/5/2022 19:21:20 -06:00		n1_clus2		n2_clus2
none					
n2					
	3/5/2022 19:21:18 -06:00		n2_clus2		n1_clus1
none					
	3/5/2022 19:21:20 -06:00		n2_clus2		n1_clus2
none					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo llamando a un mensaje AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

El futuro

["Configure la supervisión de estado del switch".](#)

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:

- ["Switches Ethernet de Cisco"](#)
- ["Hardware Universe"](#)

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después del mantenimiento para deshabilitar la creación de casos durante la duración del mantenimiento. Consulte este artículo de la base de conocimientos ["SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#) Para más detalles.
- Habilitar el registro de sesiones para cualquier sesión CLI. Para obtener instrucciones sobre cómo habilitar el registro de sesiones, revise la sección "Registro de salida de sesión" en este artículo de la base de conocimientos. ["Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP"](#) .

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.

La cantidad de puertos de 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#).

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 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		
CL2 NX3232C	cluster-network	10.10.1.102
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
      n1_clus1      up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0a      false
      n1_clus3      up/up      10.10.0.3/24      n1
e0d      false
      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
e0a      false
      n2_clus3      up/up      10.10.0.7/24      n2
e0d      false
      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
e4a      false
      n4_clus1      up/up      10.10.0.11/24      n4
e4a      true
      n4_clus2      up/up      10.10.0.12/24      n4
e4a      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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y. network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
n1			
	3/5/2022 19:21:18 -06:00	n1_clus2	n2-clus1
none			
	3/5/2022 19:21:20 -06:00	n1_clus2	n2_clus2
none			
.			
.			
n2			
	3/5/2022 19:21:18 -06:00	n2_clus2	n1_clus1
none			
	3/5/2022 19:21:20 -06:00	n2_clus2	n1_clus2
none			
.			
.			
n3			
.			
.			
.n4			
.			
.			

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```



```

cluster1::*> cluster ping-cluster -node local
Host is 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

Status

e4a	Cluster	Cluster		up	9000	auto/40000	-

e4e	Cluster	Cluster		up	9000	auto/40000	-

-

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y. network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet			Source	Destination
Node	Date		LIF	LIF
Loss				
-----	-----	-----	-----	-----
n1				
	3/5/2022 19:21:18 -06:00		n1_clus2	n2-clus1
none				
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2
none				
.				
.				
n2				
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1
none				
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2
none				
.				
.				
n3				
.				
.				
.n4				
.				
.				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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 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
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
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
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. 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
```

El futuro

["Configure la supervisión de estado del switch".](#)

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.

Antes de empezar

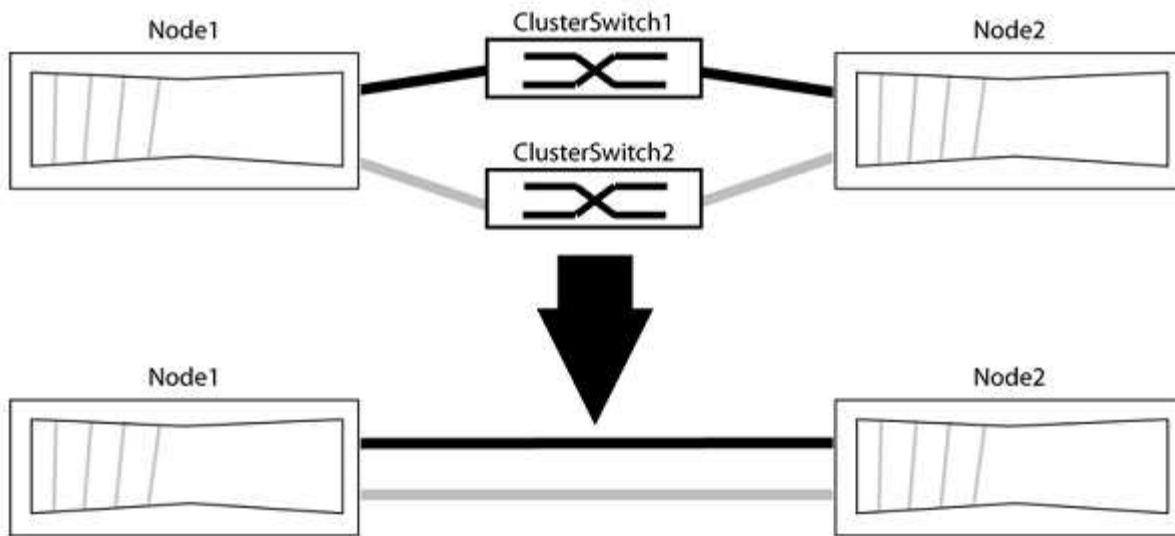
Asegúrese de tener lo siguiente:

- 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

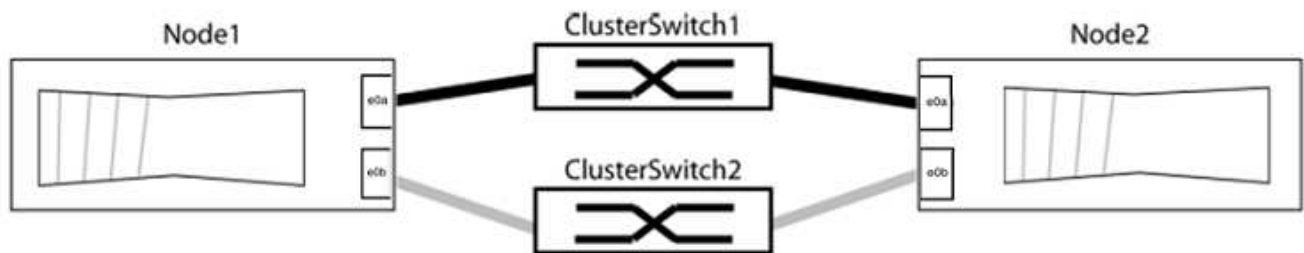
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

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 de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Verifique que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

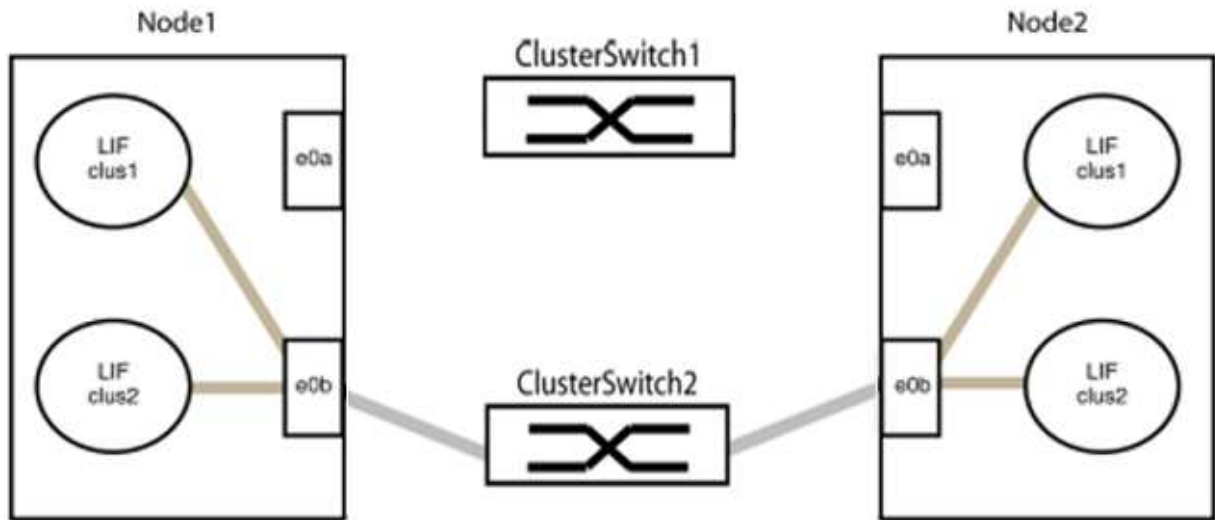
2. Configure la configuración sin switches para los puertos del grupo 1.



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**.

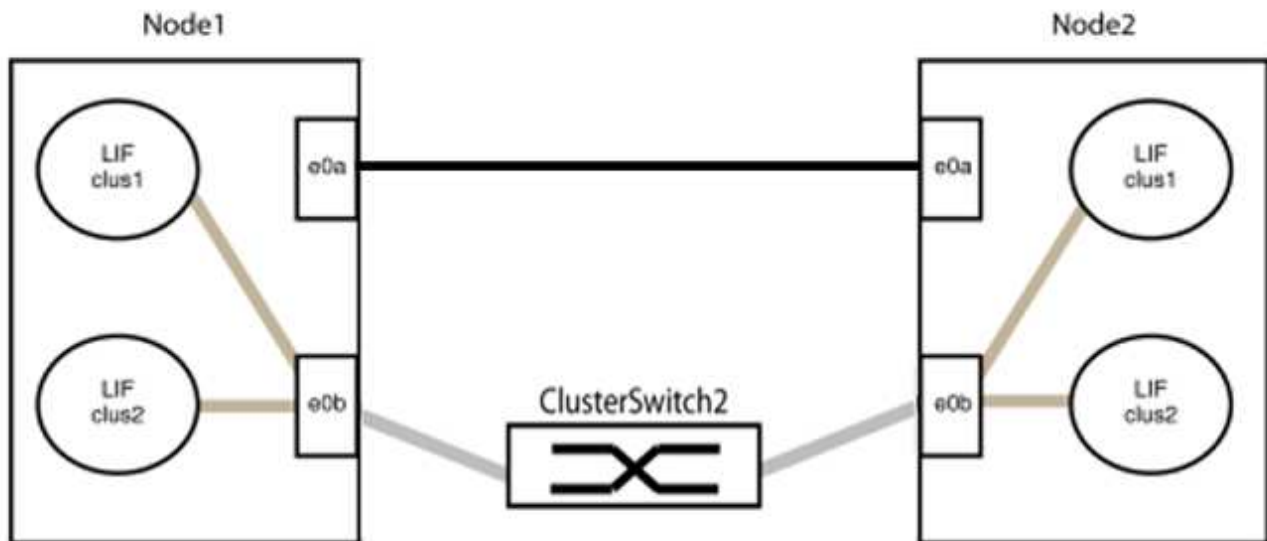
- a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

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:



3. 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
```

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y. network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```



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.

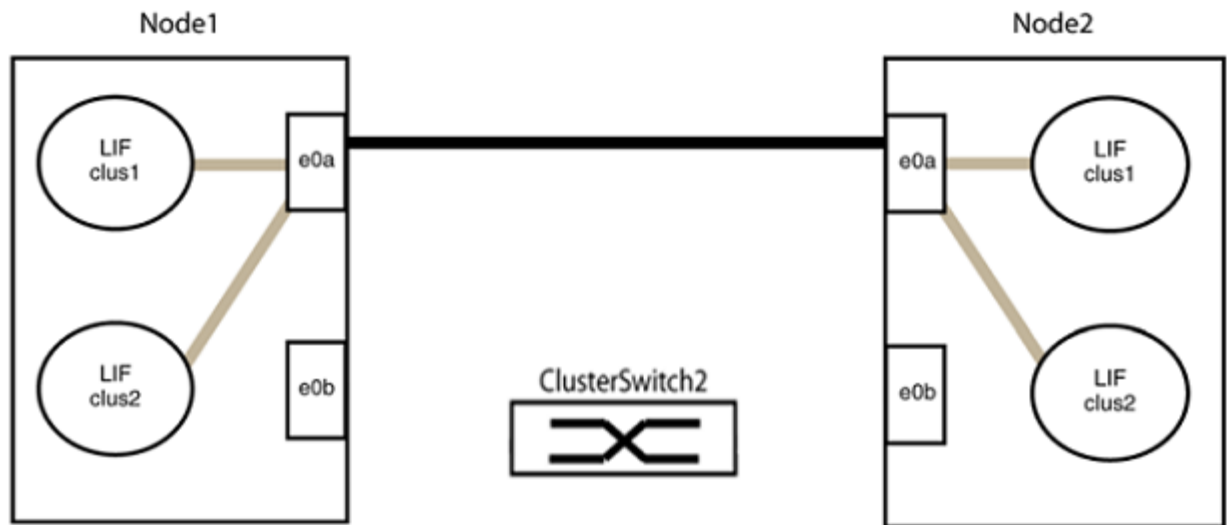
1. Configure la configuración sin switch para los puertos del grupo 2.



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 épsilon en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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"](#).

2. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

Cisco Nexus 3132Q-V

Manos a la obra

Flujo de trabajo de instalación y configuración para los conmutadores 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.

Siga estos pasos de flujo de trabajo para instalar y configurar su conmutador Cisco Nexus 3132Q-V.

1

"Requisitos de configuración"

Revise los requisitos de configuración para el conmutador de clúster 3132Q-V.

2

"Documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores 3132Q-V y el clúster ONTAP .

3

"Requisitos de Smart Call Home"

Revise los requisitos de la función Cisco Smart Call Home, que se utiliza para monitorear los componentes de hardware y software de su red.

4

"Instale el hardware"

Instale el hardware del interruptor.

5

"Configurar el software"

Configurar el software del conmutador.

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.

¿Qué sigue?

["Documentación requerida"](#) .

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.
<i>Notas de la versión de Cisco Nexus serie 3000 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 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 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 Smart Call Home, debe configurar un conmutador de red de clúster para comunicarse mediante correo electrónico con el sistema Smart Call Home. Además, puede configurar opcionalmente su conmutador de red de clúster para aprovechar la función de soporte Smart Call Home integrada de Cisco.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Antes de poder utilizar Smart Call Home, tenga en cuenta los siguientes requisitos:

- Debe haber un servidor de correo electrónico.
- 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

Flujo de trabajo de instalación de hardware para conmutadores Cisco Nexus 3132Q-V

Para instalar y configurar el hardware de un conmutador de clúster 3132Q-V, siga estos pasos:

1

"Complete la hoja de trabajo 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.

2

"Instale el interruptor"

Instale el interruptor 3132Q-V.

3

"Instale el interruptor en un armario NetApp"

Instale el conmutador 3132Q-V y el panel de paso en un gabinete NetApp según sea necesario.

4

"Revisar el cableado y la configuración"

Revise el soporte para puertos Ethernet NVIDIA .

Instalar el interruptor del grupo 3132Q-V

Siga este procedimiento para instalar y configurar el conmutador Cisco Nexus 3132Q-V.

Antes de empezar

Asegúrese de tener lo siguiente:

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones 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.
- Las licencias aplicables, la información de configuración y red, y los cables.
- Terminado ["hojas de datos para el cableado"](#) .
- Los RCF de red de gestión y red de clúster de NetApp aplicables descargados del sitio de soporte de

NetApp en "mysupport.netapp.com". 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.

- "[Documentación necesaria sobre el switch y ONTAP](#)".

Pasos

1. Monte en rack la red del clúster y los switches de red de gestión y las controladoras.

Si está instalando...	Realice lo siguiente...
Cisco Nexus 9336C-FX2 en un armario de sistemas 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.
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.

El futuro

Opcionalmente, puedes "[Instalar un conmutador Cisco Nexus 3132Q-V en un gabinete NetApp](#)". De lo contrario, vaya a "[Revisar el cableado y la configuración](#)".

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.

Antes de empezar

- 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).

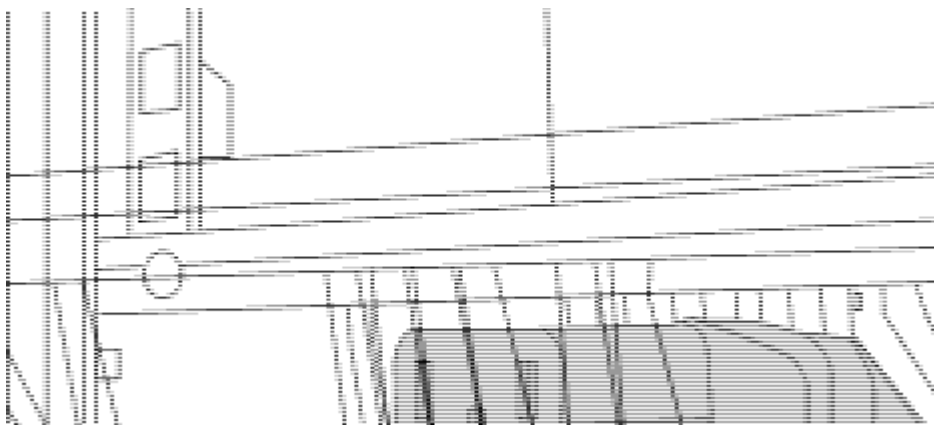
Pasos

1. Instale el panel de borrado de paso en el armario de NetApp.

- a. 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.

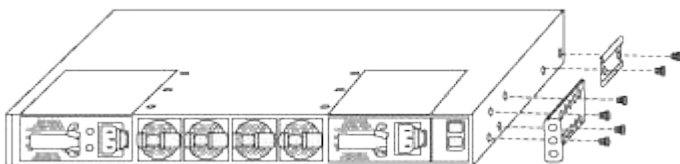
- b. Instale dos tuercas de abrazadera a cada lado en los orificios cuadrados adecuados para los rieles delanteros del armario.
- c. Centre el panel verticalmente para evitar intrusiones en el espacio adyacente del bastidor y, a continuación, apriete los tornillos.
- d. Inserte los conectores hembra de ambos cables puente de 48 pulgadas desde la parte posterior del panel y a través del conjunto del cepillo.



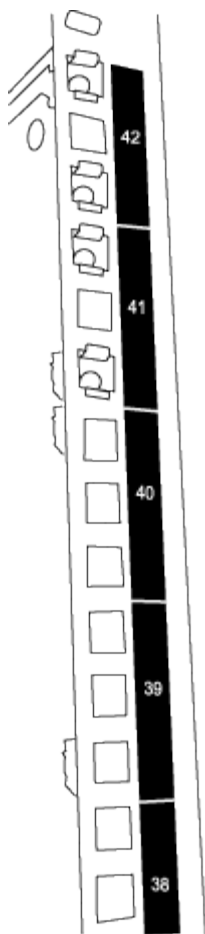
(1) conector hembra del cable puente.

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.



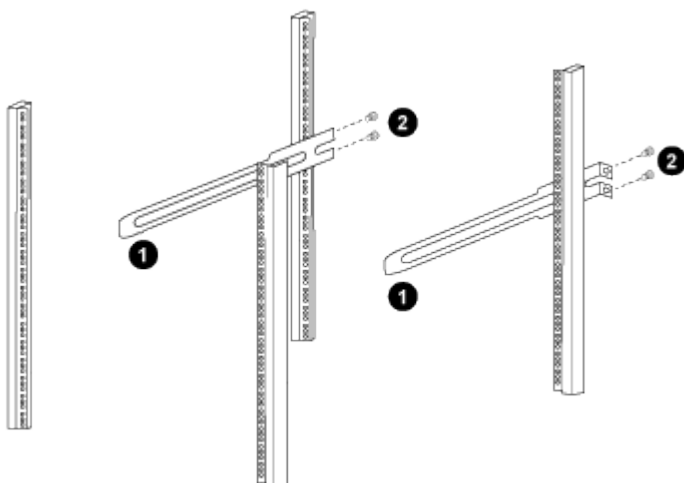
- b. Repita el paso 2a con el otro soporte de montaje en bastidor delantero en el otro lado del interruptor.
 - c. Instale el soporte de montaje en bastidor trasero en el chasis del interruptor.
 - d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del interruptor.
3. 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.

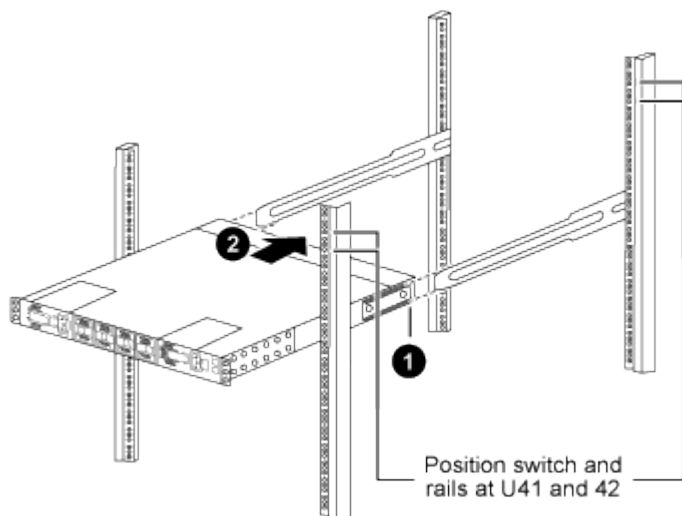
(2) apriete los tornillos de las guías deslizantes a los postes del armario.

- 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.

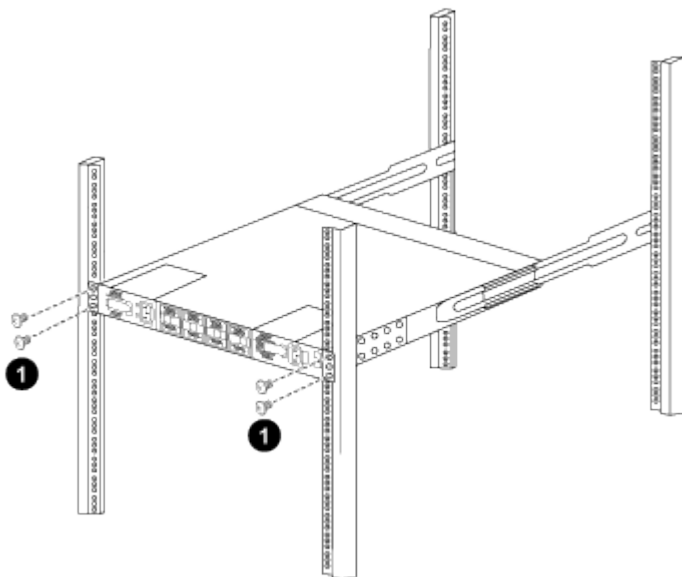
- a. Coloque la parte posterior del interruptor en RU41.



(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
(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

Flujo de trabajo de instalación de software para conmutadores de clúster Cisco Nexus 3132Q-V

Para instalar y configurar el software de un conmutador Cisco Nexus 3132Q-V e instalar o actualizar el archivo de configuración de referencia (RCF), siga estos pasos:



"Configure el switch"

Configurar el conmutador de clúster 3132Q-V.

2

"Prepárese para instalar el software NX-OS y RCF"

El software Cisco NX-OS y RCF deben estar instalados en los conmutadores de clúster Cisco 3132Q-V.

3

"Instale o actualice el software NX-OS"

Descargue e instale o actualice el software NX-OS en el conmutador de clúster Cisco 3132Q-V.

4

"Instale el RCF"

Instale el RCF después de configurar el conmutador Cisco 3132Q-V por primera vez.

5

"Compruebe la configuración de SSH"

Verifique que SSH esté habilitado en los conmutadores para usar el Monitor de estado del conmutador Ethernet (CSHM) y las funciones de recopilación de registros.

6

"Restablecer el interruptor a los valores predeterminados de fábrica"

Borre la configuración del interruptor del grupo 3132Q-V.

Configure el switch Cisco Nexus 3132Q-V.

Siga este procedimiento para configurar el switch Cisco Nexus 3132Q-V.

Antes de empezar

- 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.
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 la hoja de datos de cableado completada, como se describe en ["Hoja de trabajo completa del cableado Cisco Nexus 3132Q-V."](#)
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

Prompt	Respuesta
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
¿Habilitar el servicio telnet? (sí/no)	Responda con no . El valor predeterminado es no
¿Servicio SSH habilitado? (sí/no)	Responda con sí. El valor predeterminado es yes.  Se recomienda SSH cuando se utiliza Ethernet Switch Health Monitor (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.
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.

Prompt	Respuesta
¿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)	 Si no guarda la configuración en esta fase, ninguno de los cambios se aplicará la próxima vez que reinicie el conmutador. Responda con sí para guardar la configuración. De esta forma se actualizan automáticamente las imágenes kickstart y del sistema.

- 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 el software NX-OS

Siga este procedimiento para instalar el software NX-OS en el switch de clúster Nexus 3132Q-V.

Revise los requisitos

Antes de empezar

- 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. 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::*>
```

4. Compruebe el estado administrativo y operativo de cada puerto del clúster.

a. Compruebe que todos los puertos del clúster están **up** con un 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
Status	Status				Admin/Oper
-----	-----	-----	----	----	-----
-----	-----				
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

```
Node: cluster1-02
```

```
Ignore
```

					Speed (Mbps)
Health	Health				
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	----	-----
-----	-----				
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

					Speed (Mbps)
Health	Health				
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	----	----	-----
-----	-----				
e0a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e0b	Cluster	Cluster		up	9000
healthy	false				auto/10000

```
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
```

	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			
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                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.90      N3K-
C3132Q-V
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP

cs2                                     cluster-network     10.233.205.91      N3K-
C3132Q-V
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Deshabilite la reversión automática en las LIF del clúster. Los LIF de clúster conmutan al switch del clúster asociado y permanecen allí mientras realiza el procedimiento de actualización en el switch de destino:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

6. 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.
```

7. 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#
```

8. 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#
```

9. 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 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#
```

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 -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
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
e0a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e0d	Cluster	Cluster		up	9000
healthy	false				auto/100000

8 entries were displayed.

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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-01/cdp	e0a	cs1	Ethernet1/7	N3K-
C3132Q-V	e0d	cs2	Ethernet1/7	N3K-
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N3K-
C3132Q-V	e0d	cs2	Ethernet1/8	N3K-
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N3K-
C3132Q-V	e0b	cs2	Ethernet1/1/1	N3K-
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 Model	Type	Address	
cs1	cluster-network	10.233.205.90	N3K-
C3132Q-V			
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	N3K-

```

C3132Q-V
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                  9.3(5)
  Version Source: CDP

2 entries were displayed.

```

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.

```

11. 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::*>

```

12. Repita los pasos 6 a 11 en el interruptor CS1.

13. Habilite la reversión automática en las LIF del clúster.

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

14. 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 LIF de clúster no ha regresado a sus puertos raíz, revertirla manualmente desde el nodo local:

```
network interface revert -vserver Cluster -lif <lif_name>
```

El futuro

"[Instalación del archivo de configuración de referencia \(RCF\)](#)".

Instale o actualice el RCF

Instale o actualice la descripción general del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar los conmutadores Nexus 3132Q-V por primera vez. Actualiza tu versión RCF cuando tienes

una versión existente del archivo RCF instalado en tu conmutador.

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) para obtener más información al instalar o actualizar su RCF.

Configuraciones de RCF disponibles

En la siguiente tabla se describen los CFR disponibles para diferentes configuraciones. Seleccione el RCF aplicable a su configuración.

Si quiere más información sobre el uso de VLAN y puertos específicos, consulte el banner y la sección de notas importantes de su RCF.

Nombre de RCF	Descripción
2-Cluster-HA-Breakout	Admite dos clústeres ONTAP con al menos ocho nodos, incluidos los nodos que utilizan puertos compartidos Cluster+HA.
4-Cluster-HA-Breakout	Admite cuatro clústeres ONTAP con al menos cuatro nodos, incluidos los nodos que utilizan puertos compartidos Cluster+HA.
1-Cluster-HA	Todos los puertos están configurados para 40/100GbE. Admite el tráfico de clúster/alta disponibilidad compartido en los puertos. Necesario para los sistemas AFF A320, AFF A250 y FAS500f. Además, todos los puertos se pueden utilizar como puertos de clúster dedicados.
1-Cluster-HA-Breakout	Los puertos se configuran para 4 puertos de separación de 10 GbE, 4 GbE (RCF 1,6+ en switches 100GbE) y 40/100GbE. Admite el tráfico compartido de clúster/alta disponibilidad en los puertos para los nodos que utilizan puertos de clúster/alta disponibilidad compartidos: Sistemas AFF A320, AFF A250 y FAS500f. Además, todos los puertos se pueden utilizar como puertos de clúster dedicados.
Cluster-HA-Storage	Los puertos se configuran para 40/100GbE para clúster+HA, 4 puertos separados de 10 GbE para clúster y 4 GbE para clúster+HA, y 100GbE para cada par de alta disponibilidad de almacenamiento.
Clúster	Dos variantes de RCF con diferentes asignaciones de 4 puertos 10 GbE (breakout) y de puertos 40/100GbE. Todos los nodos FAS/AFF son compatibles, excepto para los sistemas AFF A320, AFF A250 y FAS500f.
Reducida	Todos los puertos se configuran para conexiones de almacenamiento NVMe de 100GbE Gb.

Documentación sugerida

- ["Switches Ethernet de Cisco \(NSS\)"](#)

Consulte la tabla de compatibilidad de switches para conocer las versiones de ONTAP y RCF compatibles en el sitio de soporte de NetApp. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis del comando en el RCF y la sintaxis encontrada en versiones específicas de NX-OS.

- ["Switches Cisco Nexus serie 3000"](#)

Consulte las guías de software y actualización correspondientes disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación del conmutador Cisco.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos interruptores Cisco son **CS1** y **CS2**.
- Los nombres de los nodos son **cluster1-01**, **cluster1-02**, **cluster1-03** y **cluster1-04**.
- Los nombres de LIF de los clústeres son **cluster1-01_clus1**, **cluster1-04_clus2**, **cluster1-03_clus2**, **cluster1-03_clus1**, **cluster1-02_clus2**, **cluster1-02_clus1**, **cluster1-01_clus1** y **cluster1-04_clus1**.
- La `cluster1 : *` prompt indica el nombre del clúster.

En los ejemplos de este procedimiento se utilizan cuatro nodos. Estos nodos utilizan dos puertos de interconexión de clúster 10GbE **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.

Para obtener detalles de las configuraciones RCF disponibles, consulte ["Flujo de trabajo de instalación del software"](#).

Comandos utilizados

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 futuro

Después de haber revisado el procedimiento de instalación o actualización de RCF, ["instalar el RCF"](#) o ["Mejora tu RCF"](#) según sea necesario.

Instalación del archivo de configuración de referencia (RCF)

Instale el archivo de configuración de referencia (RCF) después de configurar los conmutadores Nexus 3132Q-V por primera vez.

Antes de empezar

Compruebe las siguientes instalaciones y conexiones:

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El RCF actual.
- Una conexión de consola al conmutador, necesaria para instalar el RCF.

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.

No se necesita ningún enlace entre conmutadores (ISL) operativo durante este procedimiento. Esto es así por

diseño porque los cambios de versión de RCF pueden afectar la conectividad de ISL temporalmente. Para habilitar operaciones de clúster sin interrupciones, el siguiente procedimiento migra todos los LIF del clúster al conmutador del socio operativo mientras se realizan los pasos en el conmutador de destino.

Paso 1: Instale el RCF en los interruptores

- 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
```

Speed (Mbps)

```

Health   Health
Port     IPspace   Broadcast Domain Link MTU   Admin/Oper
Status   Status
-----
e0a      Cluster   Cluster           up    9000   auto/10000
healthy  false
e0b      Cluster   Cluster           up    9000   auto/10000
healthy  false
cluster1::*>

```

b. 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> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit

```



La cantidad de puertos mostrados varía según la cantidad de nodos del clúster.

- Verifique que los puertos del clúster hayan conmutado por error a los puertos alojados en el conmutador de clúster cs1. Esto podría tardar unos segundos.

```
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	169.254.3.4/23	
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::*>				

- 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::*>
```

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. Registre cualquier adición personalizada entre la configuración en ejecución actual y el archivo RCF en uso.



Asegúrese de configurar lo siguiente: * Nombre de usuario y contraseña * Dirección IP de administración * Puerta de enlace predeterminada * Nombre del conmutador

9. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.



Al actualizar o aplicar un nuevo RCF, debe borrar la configuración del interruptor y realizar la configuración básica. Debe estar conectado al puerto de consola serie del conmutador para configurar el conmutador nuevamente.

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

10. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

```
cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region racl 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region e-racl 256" >>
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region qos 256" >>
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) Para más detalles.

11. Verificar que el write_erase.cfg El archivo se completa como se esperaba:

```
show file bootflash:write_erase.cfg
```

12. Emitir el write erase Comando para borrar la configuración guardada actual:

```
cs2# write erase
```

```
Warning: This command will erase the startup-configuration.
```

```
Do you wish to proceed anyway? (y/n) [n] y
```

13. Copie la configuración básica guardada anteriormente en la configuración de inicio.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

14. Reinicie el switch:

```
cs2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

15. Repita los pasos 7 a 14 en el interruptor cs1.
16. Conecte los puertos de clúster de todos los nodos del clúster de ONTAP a los switches CS1 y CS2.

Paso 2: Verifique las conexiones del interruptor

1. Compruebe que los puertos del switch conectados a los puertos del clúster son **up**.

```
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::*>
```

Paso 3: Configure su clúster ONTAP

NetApp recomienda usar System Manager para configurar clústeres nuevos.

System Manager proporciona un flujo de trabajo simple y fácil para la configuración y el establecimiento de un clúster, incluida la asignación de una dirección IP de administración de nodo, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento de almacenamiento inicial.

Referirse a ["Configure ONTAP en un nuevo clúster con System Manager"](#) para obtener instrucciones de configuración.

El futuro

Después de haber instalado el RCF, ["verificar la configuración de SSH"](#) .

Actualice su archivo de configuración de referencia (RCF)

Actualice la versión de RCF cuando tenga instalada una versión existente del archivo RCF en los conmutadores operativos.

Antes de empezar

Asegúrese de tener lo siguiente:

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El RCF actual.
- Si está actualizando la versión de RCF, necesita una configuración de inicio en el RCF que refleje las imágenes de inicio deseadas.

Si necesita cambiar la configuración 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.



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.



Antes de instalar una nueva versión de software del conmutador y RCF, debe borrar los ajustes del conmutador y realizar la configuración básica. Debe estar conectado al switch mediante la consola serie o haber conservado la información básica de configuración antes de borrar la configuración del switch.

Paso 1: Prepárese para la actualización

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.

Paso 2: Configurar puertos

1. En el switch de clúster cs2, apague los puertos conectados a los puertos del clúster de los nodos.

```

cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit

```



La cantidad de puertos mostrados varía según la cantidad de nodos del clúster.

2. Verifique que los puertos del clúster hayan conmutado por error a los puertos alojados en el conmutador de clúster cs1. Esto podría tardar unos segundos.

```
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	169.254.3.4/23	
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::*>				

3. 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::*>
```

4. 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
```

5. Registre cualquier adición personalizada entre la configuración en ejecución actual y el archivo RCF en uso.

Asegúrese de configurar lo siguiente:



- Nombre de usuario y contraseña
- Dirección IP de gestión
- Puerta de enlace predeterminada
- Cambiar nombre

6. Guarde los detalles básicos de configuración en `write_erase.cfg` archivo en el bootflash.



Al actualizar o aplicar un nuevo RCF, debe borrar la configuración del interruptor y realizar la configuración básica. Debe estar conectado al puerto de consola serie del conmutador para configurar el conmutador nuevamente.

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
```

```
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
```

```
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
```

```
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

7. Para la versión 1.12 y posteriores de RCF, ejecute los siguientes comandos:

```
cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
```

```
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region racl 256" >>  
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region e-racl 256" >>  
bootflash:write_erase.cfg
```

```
cs2# echo "hardware access-list tcam region qos 256" >>  
bootflash:write_erase.cfg
```

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) Para más detalles.

8. Verificar que el `write_erase.cfg` El archivo se completa como se esperaba:

```
show file bootflash:write_erase.cfg
```

9. Emitir el `write erase` Comando para borrar la configuración guardada actual:

```
cs2# write erase
```

```
Warning: This command will erase the startup-configuration.
```

```
Do you wish to proceed anyway? (y/n) [n] y
```

10. Copie la configuración básica guardada anteriormente en la configuración de inicio.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

11. Reinicie el switch:

```
cs2# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

12. Cuando se pueda volver a acceder a la dirección IP de administración, inicie sesión en el switch a través de SSH.

Es posible que necesite actualizar las entradas del archivo host relacionadas con las claves SSH.

13. Copie el RCF al bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información sobre los comandos de Cisco , consulte la guía correspondiente en ["Referencia de comandos 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)...
```

14. 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
```



Asegúrese de leer detenidamente las secciones **Notas de instalación**, **Notas importantes** y **banner** de su RCF. Debe leer y seguir estas instrucciones para garantizar la configuración y el funcionamiento adecuados del conmutador.

15. 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 poner en línea sus puertos 10GbE después de una actualización del RCF, consulte el artículo de la Base de conocimientos ["Los puertos 10GbE de un switch de clúster Cisco 3132Q no se conectan"](#) .

16. Después de verificar que las versiones de RCF y las configuraciones de los conmutadores sean correctas, copie el archivo running-config archivo al startup-config archivo.

Para obtener más información sobre 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
```

17. Reinicie el interruptor CS2. Puede ignorar los dos eventos de «puertos del clúster inactivos» que se informan en los nodos mientras el switch se reinicia y el resultado del error % Invalid command at '^' marker.

```
cs2# reload  
This command will reboot the system. (y/n)? [n] y
```

18. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.
19. 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
```

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: cluster1-02
```

```
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: cluster1-03
```

```
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					

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.

20. En el switch de clúster cs1, apague los puertos conectados a los puertos del clúster de los nodos.

Muestra el ejemplo

```

cs1> enable
cs1# configure
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1# exit

```



La cantidad de puertos mostrados varía según la cantidad de nodos del clúster.

21. 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::*>				

22. 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::*>
```

23. Repita los pasos 1 a 19 en el interruptor cs1.
24. Habilite la reversión automática en las LIF del clúster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert True
```

25. 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. Verifique que los LIF del clúster hayan regresado a sus puertos de origen:

```
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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
-----	-----	-----
cluster1-01		
3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-02_clus2
none		
cluster1-02		
3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-01_clus1
none		
3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-01_clus2
none		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is 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)

```

El futuro

Después de haber actualizado su RCF, ["verificar la configuración de SSH"](#) .

Compruebe su configuración SSH

Si utiliza la supervisión de estado del switch Ethernet (CSHM) y las funciones de recogida de registros, compruebe que las claves SSH y SSH estén habilitadas en los switches de clústeres.

Pasos

1. Compruebe que SSH está habilitado:

```

(switch) show ssh server
ssh version 2 is enabled

```

2. Compruebe que las claves SSH estén habilitadas:

```
show ssh key
```

Muestra el ejemplo

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yIPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDsrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(switch)# show feature | include scpServer
scpServer          1          enabled
(switch)# show feature | include ssh
sshServer          1          enabled
(switch)#
```



Al habilitar FIPS, debe cambiar el bitcount a 256 en el conmutador mediante el comando `ssh key ecdsa 256 force`. Consulte ["Configurar la seguridad de red con FIPS"](#) para obtener más información.

El futuro

["Configure la supervisión de estado del switch"](#).

Restablecer el interruptor del grupo 3132Q-V a los valores predeterminados de fábrica

Para restablecer el interruptor del grupo 3132Q-V a los valores predeterminados de fábrica, debe borrar la configuración del interruptor 3132Q-V.

Acerca de esta tarea

- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Borrar la configuración existente:

```
write erase
```

```
(cs2)# write erase
```

```
Warning: This command will erase the startup-configuration.  
Do you wish to proceed anyway? (y/n) [n] y
```

2. Recargue el software del conmutador:

```
reload
```

```
(cs2)# reload
```

```
This command will reboot the system. (y/n)? [n] y
```

El sistema se reinicia y entra en el asistente de configuración. Durante el arranque, si recibe el mensaje “¿Desea cancelar el aprovisionamiento automático y continuar con la configuración normal?” (sí/no)[n]”, debe responder **sí** para continuar.

Migrar switches

Migración de switches de CN1610 GbE

Migre de switches CN1610 al flujo de trabajo de switches Nexus 3132Q-V.

Siga estos pasos del flujo de trabajo para migrar los switches CN1610 a Cisco los switches Nexus 3132Q-V.

1

"Requisitos de migración"

Revise los requisitos y la información del switch de ejemplo para el proceso de migración.

2

"Prepare la migración"

Prepare los switches CN1610 para la migración a los switches Nexus 3132Q-V.

3

"Configure los puertos"

Configure sus puertos para la migración a los nuevos switches Nexus 3132Q-V.

4

"Completa la migración"

Complete la migración a los nuevos switches de Nexus 3132Q-V.

Requisitos de migración

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.



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 NetApp CN1601 y CN1610"](#)
- ["Página de descripción de Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Requisitos del CN1610

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.

Acerca de los ejemplos utilizados

En los ejemplos de este procedimiento, se describen el reemplazo de switches CN1610 por Cisco switches Nexus 3132Q-V. Puede usar estos pasos (con modificaciones) para otros switches Cisco más antiguos.

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 CN1610 interruptores que se van a sustituir son **CL1** y **CL2**.
- Los switches Nexus 3132Q-V para reemplazar los interruptores CN1610 son **C1** y **C2**.
- **n1_clus1** es la primera interfaz lógica de clúster (LIF) conectada al conmutador de clúster 1 (CL1 o C1) para el nodo **n1**.
- **n1_clus2** es el primer LIF de clúster conectado al conmutador de clúster 2 (CL2 o C2) para el nodo **n1**.
- **n1_clus3** es el segundo LIF conectado al conmutador de cluster 2 (CL2 o C2) para el nodo **n1**.
- **n1_clus4** es el segundo LIF conectado al conmutador de cluster 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**.

En ["Hardware Universe"](#) la se muestran los puertos de clúster reales de las plataformas.

El futuro

["Prepare la migración"](#).

Prepárese para la migración de switches de CN1610 a switches de 3132Q-V.

Siga estos pasos para preparar los switches CN1610 para su migración a Cisco los switches Nexus 3132Q-V.

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
```

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

      Broadcast
Port  IPspace  Domain  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

      Broadcast
Port  IPspace  Domain  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.
```

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					
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 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. Ver ["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. Seleccione **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						
	n1_clus1	up/up	10.10.0.1/24	n1	e0a	
true						
	n1_clus2	up/up	10.10.0.2/24	n1	e0a	
false						
	n1_clus3	up/up	10.10.0.3/24	n1	e0d	
false						
	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	e0a	
false						
	n2_clus3	up/up	10.10.0.7/24	n2	e0d	
false						
	n2_clus4	up/up	10.10.0.8/24	n2	e0d	
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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y. network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Node	Date		Source LIF	Destination LIF	Packet Loss
n1					
	3/5/2022 19:21:18 -06:00		n1_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2	none
n2					
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2	none

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

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)

```

1. 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)#
```

2. 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
```

El futuro

["Configure los puertos"](#).

Configure sus puertos para la migración de switches de CN1610 a switches de 3132Q V.

Siga estos pasos para configurar los puertos para la migración desde los switches CN1610 a los nuevos switches Nexus 3132Q-V.

Pasos

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 de 3132Q-V C2 cuando se activan 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                                     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                                     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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y. network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Node	Date		Source LIF	Destination LIF	Packet Loss
n1					
	3/5/2022 19:21:18 -06:00		n1_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2	none
n2					
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2	none

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

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)

```

1. En cada nodo del cluster, migre las interfaces asociadas al primer switch CN1610 CL1, para ser reemplazadas:

```
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
```

2. 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.

3. 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
```

4. 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#
```

5. 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.

6. 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.

7. 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.
```

8. 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.
```

El futuro

"Completa la migración".

Complete la migración de los switches CN1610 a los switches Nexus 3132Q-V.

Complete los siguientes pasos para finalizar la migración de switches CN1610 a los switches Nexus 3132Q-V.

Pasos

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      Health      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      Health      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						
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.

6. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y. network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Node	Date		Source LIF	Destination LIF	Packet Loss
n1					
	3/5/2022 19:21:18 -06:00		n1_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00		n1_clus2	n2_clus2	none
n2					
	3/5/2022 19:21:18 -06:00		n2_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00		n2_clus2	n1_clus2	none

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

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)

```

1. Amplía el cluster agregando nodos a los switches de cluster Nexus 3132Q-V.
2. 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

		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.

3. 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
```

4. 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
```

5. 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.

6. 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
```

El futuro

["Configure la supervisión de estado del switch".](#)

Migración del switch Cisco Nexus 5596

Migre de switches Nexus 5596 al flujo de trabajo de switches Nexus 3132Q-V.

Siga estos pasos del flujo de trabajo para migrar los switches Cisco Nexus 5596 a los switches Cisco Nexus 3132Q-V.

1

"Requisitos de migración"

Revise los requisitos y la información del switch de ejemplo para el proceso de migración.

2

"Prepare la migración"

Prepare los switches Nexus 5596 para la migración a los switches Nexus 3132Q-V.

3

"Configure los puertos"

Configure sus puertos para la migración a los nuevos switches Nexus 3132Q-V.

4

"Completa la migración"

Complete la migración a los nuevos switches de Nexus 3132Q-V.

Requisitos de migración

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.



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:

- ["Switch Ethernet de Cisco"](#)
- ["Hardware Universe"](#)

Requisitos de Cisco Nexus 5596

Los switches de clúster utilizan los siguientes puertos para las conexiones a los nodos:

- Nexus 5596: Puertos E1/1-40 (10 GbE)
- Nexus 3132Q-V: Puertos E1/1-30 (10/40/100 GbE)

Los switches de clúster utilizan los siguientes puertos de enlace entre switches (ISL):

- Nexus 5596: Puertos E1/41-48 (10 GbE)
- Nexus 3132Q-V: Puertos E1/31-32 (40/100 GbE)

El ["Hardware Universe"](#) contiene información sobre el cableado admitido para 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 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 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 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 3132Q-V son 2 puertos SFP+, que denominan 1/33 y 1/34.
- Ha configurado algunos de los puertos de los switches Nexus 3132Q-V 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 3132Q-V.
- Las versiones de ONTAP y NX-OS compatibles con este procedimiento son las siguientes: ["Switches Ethernet de Cisco"](#).

Acerca de los ejemplos utilizados

Los ejemplos de este procedimiento describen el reemplazo de los switches Cisco Nexus 5596 por switches Cisco Nexus 3132Q-V. Puede usar estos pasos (con modificaciones) para otros switches Cisco más antiguos.

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 switches Nexus 5596 a sustituir son **CL1** y **CL2**.
- Los switches Nexus 3132Q-V para reemplazar los switches Nexus 5596 son **C1** y **C2**.
- **n1_clus1** es la primera interfaz lógica de clúster (LIF) conectada al conmutador de clúster 1 (CL1 o C1) para el nodo **n1**.

- **n1_clus2** es el primer LIF de clúster conectado al conmutador de clúster 2 (CL2 o C2) para el nodo **n1**.
- **n1_clus3** es el segundo LIF conectado al conmutador de cluster 2 (CL2 o C2) para el nodo **n1**.
- **n1_clus4** es el segundo LIF conectado al conmutador de cluster 1 (CL1 o C1) para el nodo **n1**.
- La cantidad de puertos de 10 GbE y 40/100 GbE se define en los archivos de configuración de referencia (RCF) disponibles en ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#).
- 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**.

En ["Hardware Universe"](#) la se muestran los puertos de clúster reales de las plataformas.

Escenarios cubiertos

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.

El futuro

["Prepare la migración"](#).

Prepárese para la migración desde switches Nexus 5596 a switches Nexus 3132Q-V.

Siga estos pasos para preparar los switches Cisco Nexus 5596 para la migración a los switches Cisco Nexus 3132Q-V.

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`

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:

- Ir a "[Switches Ethernet de Cisco](#)" en el sitio de soporte de NetApp .
- Anote el conmutador y las versiones de software necesarias en la tabla de esa página.
- Descargue la versión adecuada del RCF.
- Seleccione **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.
- Descargue la versión adecuada del software Image.

Consulte la página *ONTAP 8.x o posterior Archivos de configuración de referencia de switch de red de administración y clúster* Download y, a continuación, seleccione 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 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.
```

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

				Source	Destination							
Packet				LIF	LIF							
Node	Date											
Loss												

n1												
	3/5/2022	19:21:18	-06:00	n1_clus2	n2_clus1	none						
	3/5/2022	19:21:20	-06:00	n1_clus2	n2_clus2	none						
n2												
	3/5/2022	19:21:18	-06:00	n2_clus2	n1_clus1	none						
	3/5/2022	19:21:20	-06:00	n2_clus2	n1_clus2	none						

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

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)

```

1. Apague los puertos ISL 41 a 48 en el switch Nexus 5596 activo 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.

2. 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
```

El futuro

"Configure los puertos".

Configure sus puertos para la migración de switches de 5596 a switches de 3132Q V.

Siga estos pasos para configurar los puertos para la migración desde los switches Nexus 5596 a los nuevos switches Nexus 3132Q-V.

Pasos

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

				Source	Destination							
Packet				LIF	LIF							
Node	Date											
Loss												

n1												
	3/5/2022	19:21:18	-06:00	n1_clus2	n2_clus1	none						
	3/5/2022	19:21:20	-06:00	n1_clus2	n2_clus2	none						
n2												
	3/5/2022	19:21:18	-06:00	n2_clus2	n1_clus1	none						
	3/5/2022	19:21:20	-06:00	n2_clus2	n1_clus2	none						

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

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)

```

1. En cada nodo del cluster, migre las interfaces asociadas con el primer switch Nexus 5596, CL1, para ser reemplazado:

```
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
```

2. 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.

-----
```

3. 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
```

4. 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#
```

5. 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.

6. 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.

7. 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.

```

8. 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.

```

El futuro

["Completa la migración"](#).

Complete la migración de los switches Nexus 5596 a los switches Nexus 3132Q-V.

Complete los siguientes pasos para finalizar la migración de los switches Nexus 5596 a los switches Nexus 3132Q-V.

Pasos

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y. network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

				Source	Destination				
Packet				LIF	LIF				
Node	Date								
Loss									

n1									
	3/5/2022	19:21:18	-06:00	n1_clus2	n2_clus1	none			
	3/5/2022	19:21:20	-06:00	n1_clus2	n2_clus2	none			
n2									
	3/5/2022	19:21:18	-06:00	n2_clus2	n1_clus1	none			
	3/5/2022	19:21:20	-06:00	n2_clus2	n1_clus2	none			

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

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)

```

1. Amplía el cluster agregando nodos a los switches de cluster Nexus 3132Q-V.
2. 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.

3. 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
```

4. 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
```

5. 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.

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
```

El futuro

["Configure la supervisión de estado del switch".](#)

Migre de clústeres sin switch a clústeres con switches de dos nodos

Migre desde clústeres sin switch al flujo de trabajo de clústeres con switches de dos nodos

Siga estos pasos del flujo de trabajo para migrar desde un clúster sin switches de dos nodos a un clúster con switches Cisco de dos nodos que incluya los switches de red de clúster Nexus 3132Q-V.

1**"Requisitos de migración"**

Revise los requisitos y la información del switch de ejemplo para el proceso de migración.

2**"Prepare la migración"**

Preparar los clústeres sin switch para la migración a clústeres con switches de dos nodos.

3**"Configure los puertos"**

Configure los puertos para la migración de clústeres de dos nodos sin switch a clústeres de dos nodos con switches de dos nodos.

4**"Completa la migración"**

Complete la migración de clústeres sin switches a clústeres con switches de dos nodos.

Requisitos de migración

Si tiene un clúster de dos nodos sin switches, revise este procedimiento para conocer los requisitos correspondientes para migrar a un clúster de dos nodos con switches.



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:

- ["NetApp CN1601 y CN1610"](#)
- ["Switch Ethernet de Cisco"](#)
- ["Hardware Universe"](#)

Conexiones de puerto y nodo

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 a clúster de 40 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 operar puertos QSFP como modos Ethernet de 40 Gb o 4x10 Gb Ethernet.

De manera predeterminada, hay 32 puertos en el modo Ethernet de 40 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 divide un puerto Ethernet de 40 Gb en puertos Ethernet de 10 Gb, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tuplas. 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 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 puertos de Nexus 3132Q-V para funcionar a 10 GbE o 40 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.

- La cantidad de puertos de 10 GbE y 40 GbE se define en los archivos de configuración de referencia (RCF) disponibles en ["Descarga del archivo de configuración de referencia del switch de red de clúster de Cisco"](#).

Antes de empezar

- 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.

["Switches Ethernet de Cisco"](#) Tiene información sobre las versiones de ONTAP y NX-OS compatibles con 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 la conectividad de 10 GbE y 40 GbE desde los nodos a los switches de clústeres Nexus 3132Q-V.

Acerca de los ejemplos utilizados

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 usando dos puertos de interconexión de clúster de 40 GbE **E4A** y **E4E**. El ["Hardware Universe"](#) tiene detalles sobre los puertos de clúster en las plataformas.

Este procedimiento cubre los siguientes escenarios:

- **n1_clus1** es la primera interfaz lógica de clúster (LIF) que se conecta al conmutador de clúster C1 para el nodo **n1**.
- **n1_clus2** es el primer LIF de clúster que se conecta al conmutador de clúster C2 para el nodo **n1**.
- **n2_clus1** es el primer LIF de clúster que se conecta al conmutador de clúster C1 para el nodo **n2**.
- **n2_clus2** es el segundo LIF de clúster que se conecta al conmutador de clúster C2 para el nodo **n2**.
- La cantidad de puertos de 10 GbE y 40 GbE se define en los archivos de configuración de referencia (RCF) disponibles en ["Descarga del archivo de configuración de referencia del switch de red de clúster de Cisco ®"](#).



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.

El futuro

["Prepare la migración"](#).

Prepárese para la migración desde clústeres sin switches a clústeres con switches

Siga estos pasos para preparar el clúster sin switch para migrarlo a un clúster de dos nodos con switches.

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
```

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
      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.
```

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. Ir a ["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. Seleccione **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. Seleccione **CONTINUAR** en la página **Descripción**, acepte el contrato de licencia y, a continuación, siga las instrucciones de la página **Descargar** para descargar el RCF.

El futuro

["Configure los puertos"](#).

Configure los puertos para la migración de clústeres sin switch a clústeres con switches

Siga estos pasos para configurar los puertos para migrar desde clústeres sin switch de dos nodos a clústeres con switches de dos nodos.

Pasos

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

				Source	Destination							
Packet				LIF	LIF							
Node	Date											
Loss												

n1												
	3/5/2022	19:21:18	-06:00	n1_clus2	n2_clus1	none						
	3/5/2022	19:21:20	-06:00	n1_clus2	n2_clus2	none						
n2												
	3/5/2022	19:21:18	-06:00	n2_clus2	n1_clus1	none						
	3/5/2022	19:21:20	-06:00	n2_clus2	n1_clus2	none						

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

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)

```

1. Desconecte el cable de E4A en el 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.

2. 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.

3. 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
```

4. 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
```

5. 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.
```

6. 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
```

7. 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.
```

8. 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

9. 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
```

10. 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
```

11. 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.
```

12. 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.

13. 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.

14. 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
```


15. 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
```

16. 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
```

17. 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.
```

18. 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.
```

El futuro

["Completa la migración"](#).

Complete la migración de clústeres de dos nodos sin switch a clústeres con switches de dos nodos

Siga estos pasos para completar la migración desde clústeres sin switch a clústeres con switches de dos nodos.

Pasos

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
```

Node	Local Port	Discovered 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
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

				Source	Destination							
Packet				LIF	LIF							
Node	Date											
Loss												

n1												
	3/5/2022	19:21:18	-06:00	n1_clus2	n2_clus1	none						
	3/5/2022	19:21:20	-06:00	n1_clus2	n2_clus2	none						
n2												
	3/5/2022	19:21:18	-06:00	n2_clus2	n1_clus1	none						
	3/5/2022	19:21:20	-06:00	n2_clus2	n1_clus2	none						

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

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)

```

1. Si suprimió la creación automática de casos, vuelva a activarla llamando a un mensaje AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

El futuro

"Configure la supervisión de estado del switch".

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.
- La cantidad de puertos de 10 GbE y 40 GbE se define en los archivos de configuración de referencia (RCF) disponibles en ["Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®"](#).

- 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 a clúster de 40 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 operar puertos QSFP como modos Ethernet de 40 Gb o 4x10 Gb Ethernet.

De manera predeterminada, hay 32 puertos en el modo Ethernet de 40 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 divide un puerto Ethernet de 40 Gb en puertos Ethernet de 10 Gb, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tuplas. 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 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 de Nexus 3132Q-V para ejecutarse a 10 GbE o 40 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 sobre la conectividad de 10 GbE y 40 GbE desde los nodos a los switches de clústeres Nexus 3132Q-V.

["Switches Ethernet de Cisco"](#) Tiene información sobre las versiones de ONTAP y NX-OS compatibles con este procedimiento.

Requisitos de Cisco Nexus 5596

- Se admiten los siguientes switches de clúster:
 - Nexus 5596
 - Nexus 3132Q-V
- La cantidad de puertos de 10 GbE y 40 GbE se define en los archivos de configuración de referencia (RCF) disponibles en ["Descarga del archivo de configuración de referencia del conmutador de red de](#)

- 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 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 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 GbE requieren módulos QSFP/QSFP28optical compatibles 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 operar puertos QSFP/QSFP28 como modos Ethernet de 40 Gigabit o Ethernet de 4 x10 Gigabit.

De manera predeterminada, hay 32 puertos en el modo Ethernet de 40 Gigabit. 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*. Al dividir un puerto Ethernet de 40 Gigabit en 10 puertos Gigabit Ethernet, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tuplas. 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 se ejecuten a 10 GbE o 40 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 la lectura de la documentación necesaria sobre la conectividad de 10 GbE y 40 GbE desde los nodos a los switches de clúster Nexus 3132Q-V.
- Las versiones de ONTAP y NX-OS compatibles con este procedimiento se encuentran en ["Switches Ethernet de Cisco"](#).

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 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 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 en clúster de 40 GbE requieren módulos ópticos QSFP/QSFP28 compatibles 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 operar puertos QSFP/QSFP28 como modos Ethernet de 40 Gb o Ethernet de 4x 10 Gb.

De manera predeterminada, hay 32 puertos en el modo Ethernet de 40 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 divide un puerto Ethernet de 40 Gb en puertos Ethernet de 10 Gb, los puertos resultantes se numeran mediante una convención de nomenclatura de 3 tuplas. 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 de los switches Nexus 3132Q-V para ejecutarse a 10 GbE o 40 GbE.

Puede dividir los primeros seis puertos en modo 4x10 GbE con el `interface breakout module 1 port 1-6 map 10g-4x` comando. Del mismo modo, puede reagrupar 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 sobre la conectividad de 10 GbE y 40 GbE desde los nodos a los switches de clústeres Nexus 3132Q-V.
- Las versiones de ONTAP y NX-OS compatibles con este procedimiento se enumeran en "[Switches Ethernet de Cisco](#)".
- Las versiones de ONTAP y FASTPATH compatibles con este procedimiento se enumeran en "[Switches CN1601 y CN1610 de NetApp](#)".

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](#)".

Antes de empezar

- La configuración de clúster y red existente tiene:
 - La infraestructura de clúster Nexus 3132Q-V es redundante y completamente funcional en ambos switches.

"[Switch Ethernet de Cisco](#)" tiene las últimas versiones de RCF y NX-OS para sus conmutadores.

- 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](#)"

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después del mantenimiento para deshabilitar la creación de casos durante la duración del mantenimiento. Consulte este artículo de la base de conocimientos "[SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado](#)" Para más detalles.
- Habilitar el registro de sesiones para cualquier sesión CLI. Para obtener instrucciones sobre cómo habilitar el registro de sesiones, revise la sección "Registro de salida de sesión" en este artículo de la base de conocimientos. "[Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP](#)".

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.
- La cantidad de puertos de 10 GbE y 40 GbE se define en los archivos de configuración de referencia (RCF) disponibles en "[Descarga del archivo de configuración de referencia del conmutador de red de clúster Cisco®](#)".
- 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
	e0d	CL1	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	CL2	Ethernet1/1/3	N3K-C3132Q-V
	e0c	CL2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	CL1	Ethernet1/1/4	N3K-C3132Q-V
n3	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3132Q-V
	e4e	CL2	Ethernet1/7	N3K-C3132Q-V
n4	/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 , consulte "[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.
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				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0a	false			
	n1_clus3	up/up	10.10.0.3/24	n1
e0d	false			
	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
e0a	false			
	n2_clus3	up/up	10.10.0.7/24	n2
e0d	false			
	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
e4a	false			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4a	false			

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Node	Date	Source LIF	Destination LIF	Packet Loss
n1				
	3/5/2022 19:21:18 -06:00	n1_clus2	n2_clus1	none
	3/5/2022 19:21:20 -06:00	n1_clus2	n2_clus2	none
n2				
	3/5/2022 19:21:18 -06:00	n2_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00	n2_clus2	n1_clus2	none
n3				
...				
...				
n4				
...				
...				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```
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)
```

1. Apague los puertos 1/31 y 1/32 en CL1 y el conmutador 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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el comando `show` para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Node	Date	Source LIF	Destination LIF	Packet Loss
n1				
	3/5/2022 19:21:18 -06:00	n1_clus2	n2_clus1	none
	3/5/2022 19:21:20 -06:00	n1_clus2	n2_clus2	none
n2				
	3/5/2022 19:21:18 -06:00	n2_clus2	n1_clus1	none
	3/5/2022 19:21:20 -06:00	n2_clus2	n1_clus2	none
n3				
...				
...				
n4				
...				
...				

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```
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 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. 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
```

El futuro

["Configure la supervisión de estado del switch"](#)

Sustituya los switches de clúster Cisco Nexus 3132Q-V por conexiones sin switches

En ONTAP 9.3 y versiones posteriores, puede migrar de un clúster con una red de clúster conmutada a uno donde dos nodos están conectados directamente.

NetApp recomienda que actualice su versión de ONTAP antes de continuar con la operación de clúster conmutado a sin conmutadores para los conmutadores Cisco Nexus 3132Q-V.



En la siguiente sección, se ofrecen más detalles:

- ["SU540: Los errores de NIC de Chelsio T6 provocan el apagado del sistema al actualizar de conmutadores de red de 40G a 100G"](#)
- ["Pánico en el nodo después de la migración de un clúster conmutado a uno sin conmutador"](#)

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.

Antes de empezar

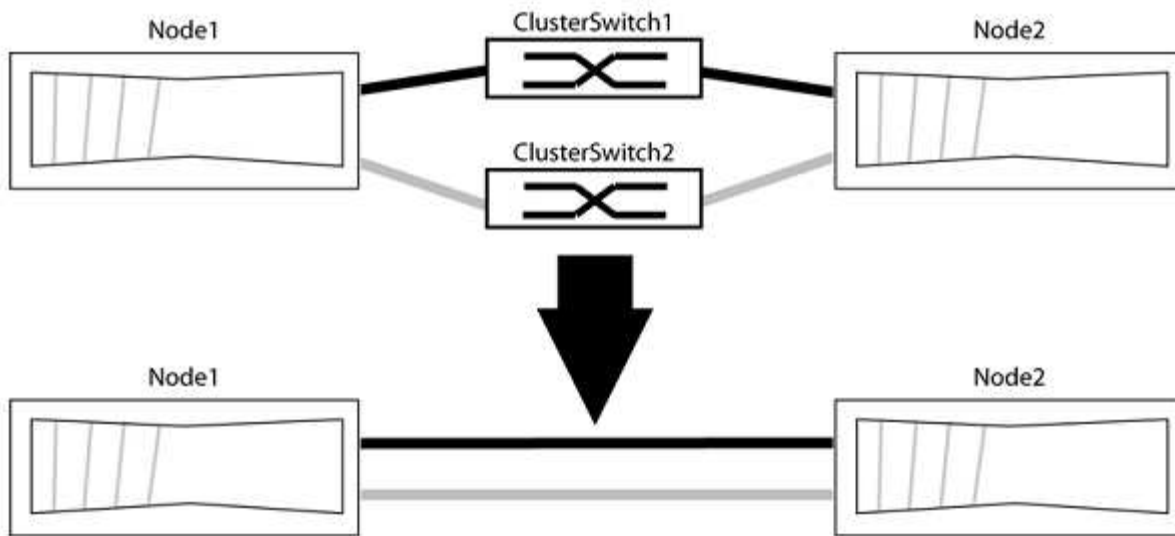
Asegúrese de tener lo siguiente:

- 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

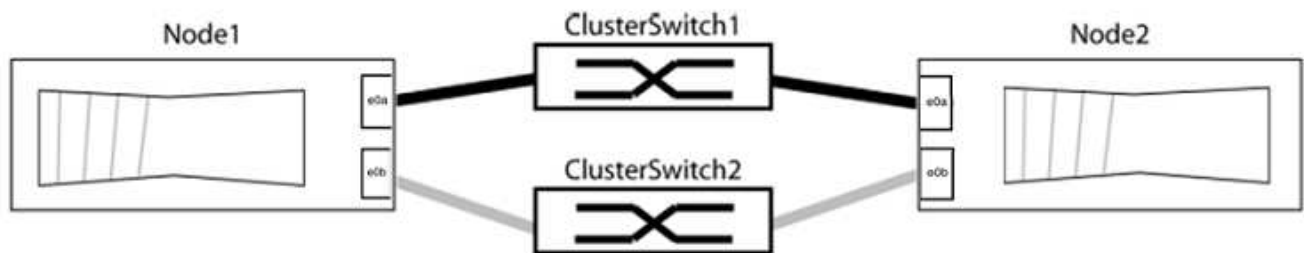
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

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 de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination					
Packet		LIF		LIF					
Node	Date								
Loss									

node1									
	3/5/2022 19:21:18 -06:00	node1_clus2		node2-clus1					
node									
	3/5/2022 19:21:20 -06:00	node1_clus2		node2_clus2					
node									
node2									
	3/5/2022 19:21:18 -06:00	node2_clus2		node1_clus1					
node									
	3/5/2022 19:21:20 -06:00	node2_clus2		node1_clus2					
node									

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Verifique que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

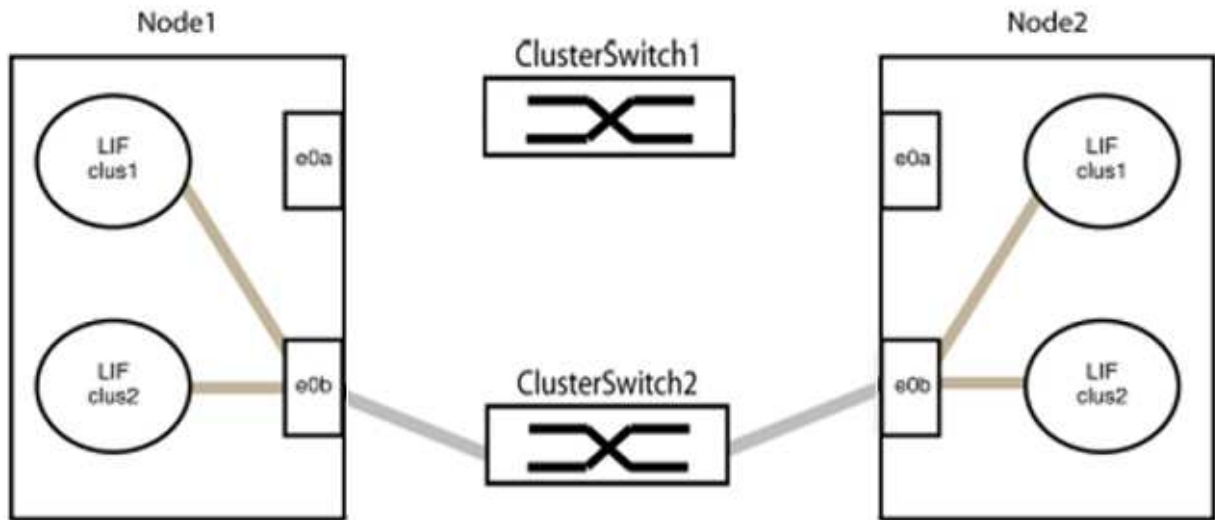
2. Configure la configuración sin switches para los puertos del grupo 1.



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**.

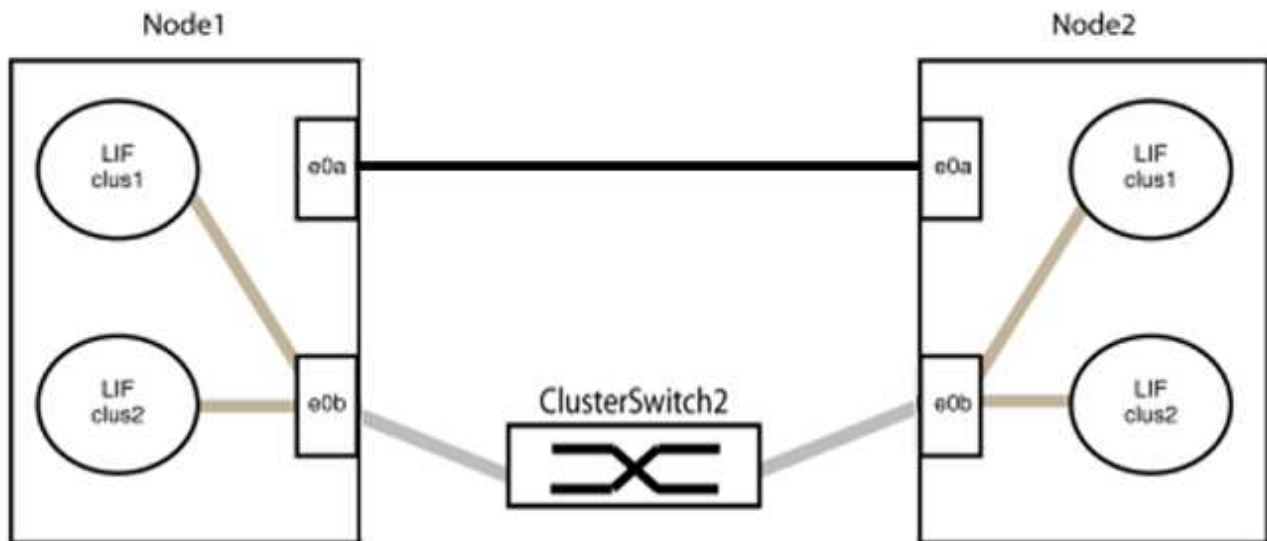
- a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

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:



3. 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
```

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node1					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node1					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node2					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node2					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```



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.

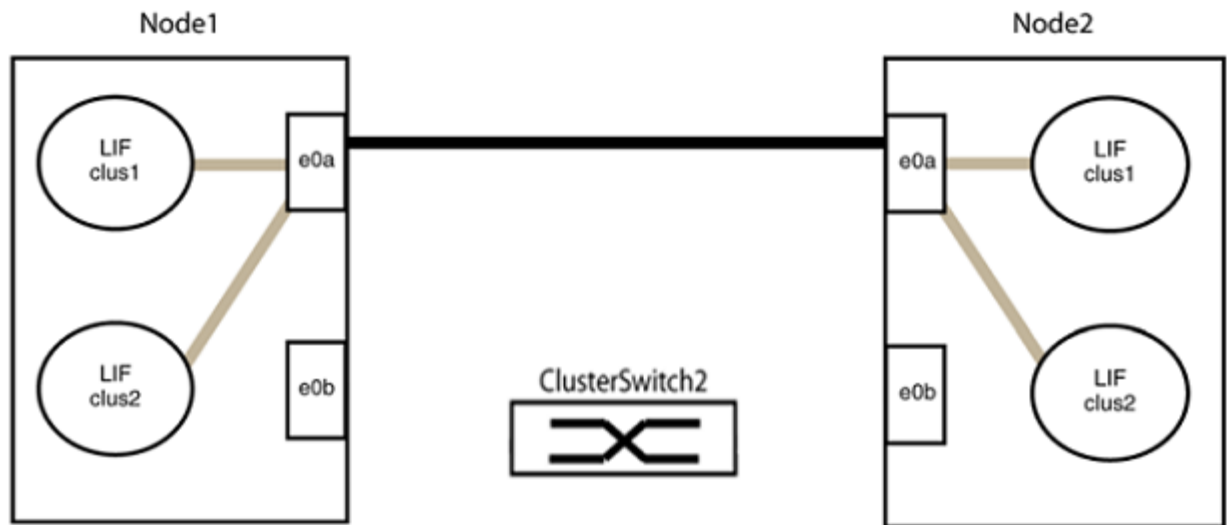
1. Configure la configuración sin switch para los puertos del grupo 2.



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**.

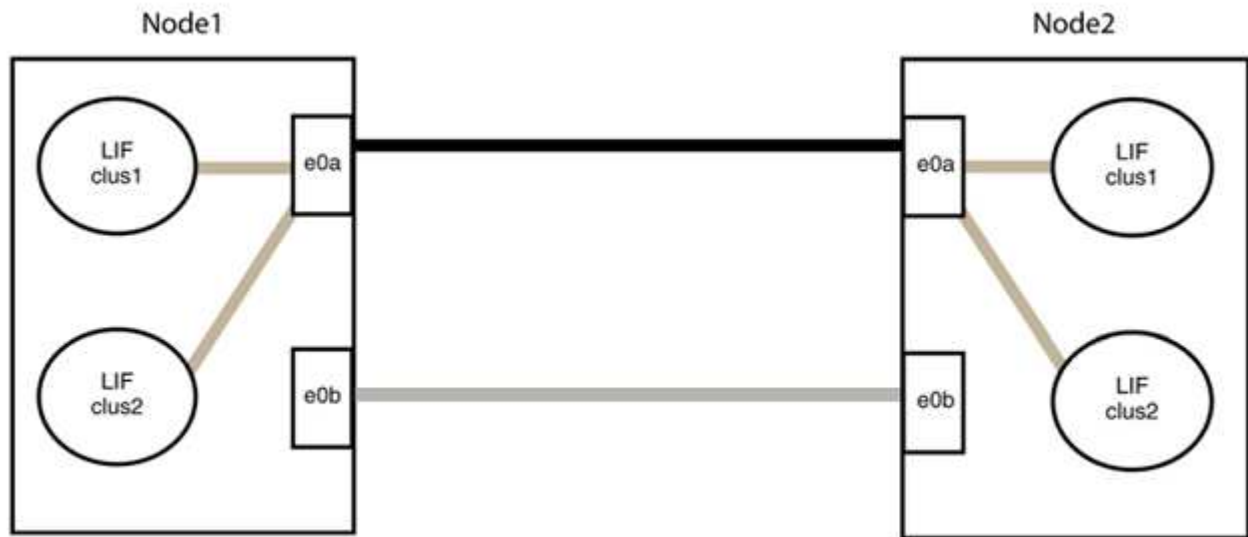
- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

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 épsilon en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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"](#).

2. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

Cisco Nexus 92300YC

Manos a la obra

Flujo de trabajo de instalación y configuración para conmutadores Cisco Nexus 92300YC

Los conmutadores Cisco Nexus 92300YC se pueden utilizar como conmutadores de clúster en su clúster AFF o FAS . Los conmutadores de clúster le permiten crear clústeres ONTAP con más de dos nodos.

Siga estos pasos de flujo de trabajo para instalar y configurar su conmutador Cisco Nexus 92300YC.

1

"Requisitos de configuración"

Revise los requisitos de configuración para el conmutador de clúster 92300YC.

2

"Documentación requerida"

Revise la documentación específica del conmutador y del controlador para configurar sus conmutadores 92300YC y el clúster ONTAP .

3

"Requisitos de Smart Call Home"

Revise los requisitos de la función Cisco Smart Call Home, que se utiliza para monitorear los componentes de hardware y software de su red.

4

"Instale el hardware"

Instale el hardware del interruptor.

5

"Configurar el software"

Configurar el software del conmutador.

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.

¿Qué sigue?

["Componentes y números de pieza"](#) .

Componentes y números de pieza de los conmutadores 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.

¿Qué sigue?

["Documentación requerida"](#) .

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 conmutadores Cisco Nexus 92300YC, necesita la siguiente documentación del ["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 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.
" Instalar un conmutador Cisco Nexus 92300YC en un gabinete 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 Smart Call Home, debe configurar un conmutador de red de clúster para comunicarse mediante correo electrónico con el sistema Smart Call Home. Además, puede configurar opcionalmente su conmutador de red de clúster para aprovechar la función de soporte Smart Call Home integrada de Cisco.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Smart Call Home monitorea los componentes de hardware y software de su red. Cuando ocurre una configuración crítica del sistema, se genera una notificación por correo electrónico y se envía una alerta a todos los destinatarios configurados en su perfil de destino.

Antes de poder utilizar Smart Call Home, tenga en cuenta los siguientes requisitos:

- Debe haber un servidor de correo electrónico.
- 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

Flujo de trabajo de instalación de hardware para conmutadores Cisco Nexus 92300YC

Para instalar y configurar el hardware de un conmutador de clúster 92300YC, siga estos pasos:

1

"Complete la hoja de trabajo 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.

2

"Instale el interruptor"

Instale el interruptor 92300YC.

3

"Instale el interruptor en un armario NetApp"

Instale el conmutador 92300YC y el panel de paso en un gabinete NetApp según sea necesario.

4

"Revisar el cableado y la configuración"

Revise el soporte para puertos Ethernet NVIDIA .

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

Switch de clúster a		Switch del clúster B	
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
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

Switch de clúster a		Switch del clúster B	
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
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

Switch de clúster a		Switch del clúster B	
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
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	
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		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	
37		37	
38		38	
39		39	
40		40	
41		41	

Switch de clúster a		Switch del clúster B	
42		42	
43		43	
44		44	
45		45	
46		46	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	

Switch de clúster a		Switch del clúster B	
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

¿Qué sigue?

["Instale el interruptor"](#) .

Instalar el interruptor de grupo 92300YC

Siga este procedimiento para configurar y configurar el switch Cisco Nexus 92300YC.

Antes de empezar

Asegúrese de tener lo siguiente:

- Acceso a un servidor HTTP, FTP o TFTP en el sitio de instalación para descargar las versiones 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.
- Las licencias aplicables, la información de configuración y red, y los cables.
- Terminado ["hojas de datos para el cableado"](#) .
- Los RCF de red de gestión y red de clúster de NetApp aplicables descargados del sitio de soporte de NetApp en ["mysupport.netapp.com"](#). 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.
- ["Documentación necesaria sobre el switch y ONTAP"](#) .

Pasos

1. Monte en rack la red del clúster y los switches de red de gestión y las controladoras.

Si está instalando...	Realice lo siguiente...
Cisco Nexus 92300YC en un gabinete de sistema NetApp	Consulte la guía _Instalación de un conmutador de clúster Cisco Nexus 92300YC y un panel de paso en un gabinete NetApp para obtener instrucciones sobre cómo instalar el conmutador en un gabinete 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.

El futuro

Opcionalmente, puedes "[Instalar un conmutador Cisco Nexus 3223C en un gabinete NetApp](#)". De lo contrario, vaya a "[Revisar el cableado y la configuración](#)".

Instalar un conmutador de clúster Cisco Nexus 92300YC en un gabinete NetApp

Dependiendo de su configuración, es posible que necesite instalar el conmutador de clúster Cisco Nexus 92300YC y el panel de paso en un gabinete NetApp con los soportes estándar que se incluyen con el conmutador.

Antes de empezar

- Los requisitos de preparación inicial, el contenido del kit y las precauciones de seguridad en el "[Guía de instalación de hardware de Cisco Nexus serie 9000](#)".
- 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.

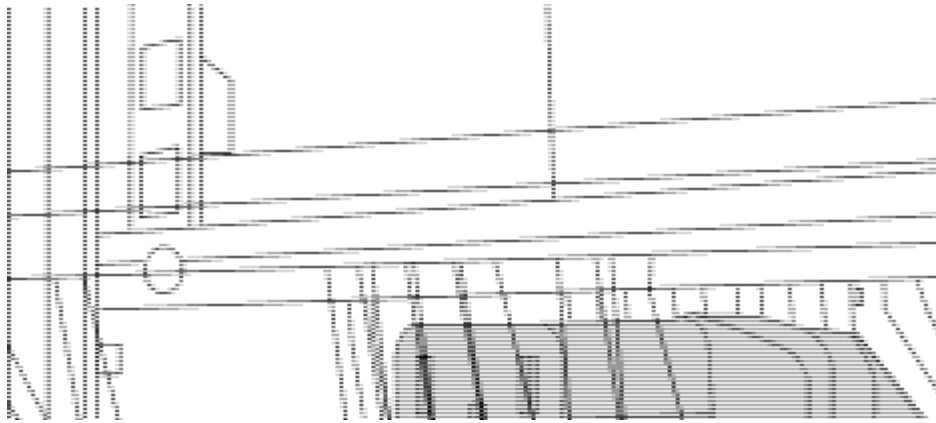
NetApp puede adquirir el kit de panel de paso a través (número de pieza X8784-R6).

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.

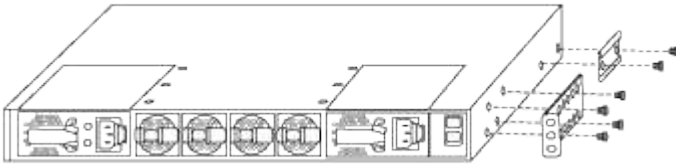
En este procedimiento, el panel de limpieza se instalará en U40.

- 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.

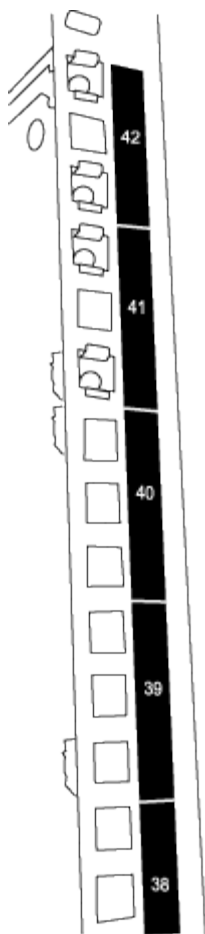


(1) *conector hembra del cable puente.*

1. Instale los soportes de montaje en rack en el chasis del conmutador Nexus 92300YC.
 - 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.



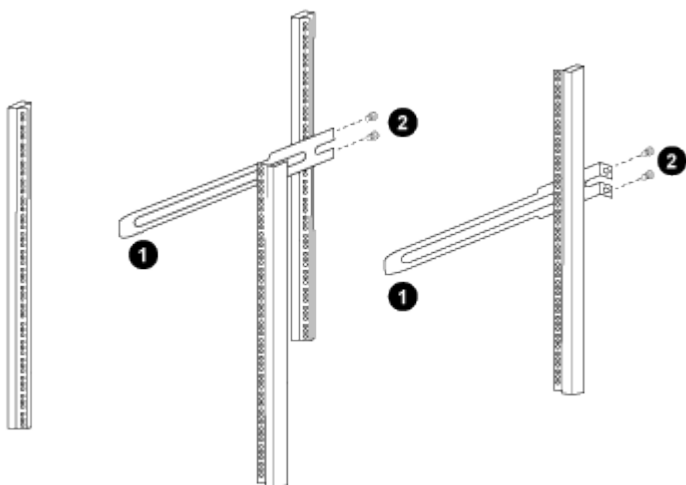
- b. Repita el paso 2a con el otro soporte de montaje en bastidor delantero en el otro lado del interruptor.
 - c. Instale el soporte de montaje en bastidor trasero en el chasis del interruptor.
 - d. Repita el paso 2c con el otro soporte de montaje en rack trasero en el otro lado del interruptor.
2. Instale las tuercas de abrazadera en las ubicaciones de los orificios cuadrados de los cuatro postes de IEA.



Los dos conmutadores 92300YC siempre se montarán en las 2U superiores del gabinete 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.



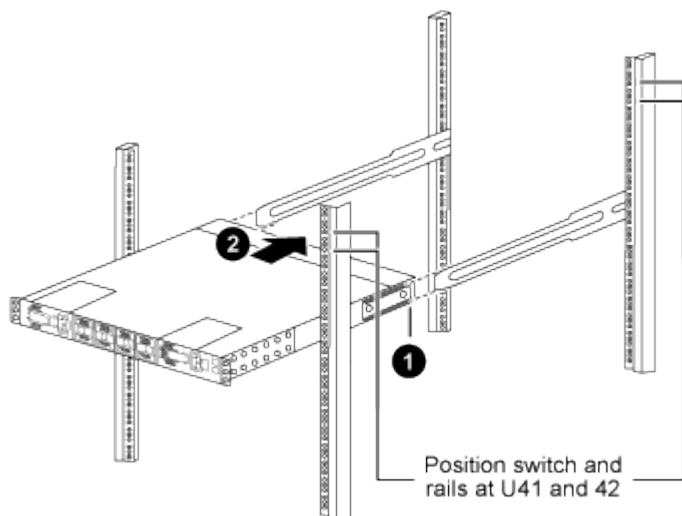
(1) mientras desliza suavemente el riel deslizante, alinéelo con los orificios de los tornillos del rack. + (2) apriete los tornillos de los rieles deslizantes a los postes del armario.

- 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.

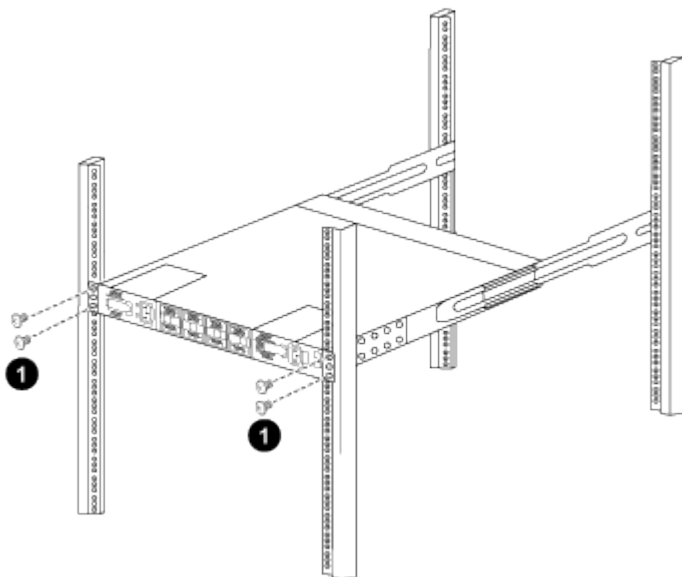
- a. Coloque la parte posterior del interruptor en RU41.



(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 administración de cada conmutador 92300YC a cualquiera de los conmutadores de administración (si se solicitaron) o conéctelos directamente a su 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 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

Flujo de trabajo de instalación de software para conmutadores de clúster Cisco Nexus 92300YC

Para instalar y configurar el software de un conmutador Cisco Nexus 92300YC e instalar o actualizar el archivo de configuración de referencia (RCF), siga estos pasos:

1**"Configure el switch"**

Configurar el conmutador de clúster 92300YC.

2**"Prepárese para instalar el software NX-OS y RCF"**

El software Cisco NX-OS y los archivos de configuración de referencia (RCF) deben estar instalados en los conmutadores de clúster Cisco 92300YC.

3**"Instale o actualice el software NX-OS"**

Descargue e instale o actualice el software NX-OS en el conmutador de clúster Cisco 392300YC.

4**"Instale el RCF"**

Instale el RCF después de configurar el conmutador Cisco 92300YC por primera vez.

5**"Compruebe la configuración de SSH"**

Verifique que SSH esté habilitado en los conmutadores para usar el Monitor de estado del conmutador Ethernet (CSHM) y las funciones de recopilación de registros.

Configure el switch Cisco Nexus 92300YC

Siga este procedimiento para configurar y configurar el switch Cisco Nexus 92300YC.

Pasos

1. Conecte el puerto serie a un host o puerto serie.
2. Conecte el puerto de gestión (en el lado que no sea un puerto del switch) a la misma red donde esté ubicado el servidor SFTP.
3. En la consola, configure los ajustes de serie del lado del host:
 - 9600 baudios
 - 8 bits de datos
 - 1 bit de parada
 - paridad: none
 - control de flujo: ninguno
4. Cuando se arranca por primera vez o se reinicia después de borrar la configuración en ejecución, el switch Nexus 92300YC recorre un ciclo de arranque. Interrumpa este ciclo escribiendo **yes** para cancelar la alimentación en el aprovisionamiento automático.

Aparecerá la configuración de la cuenta de administración del sistema.

Muestra el ejemplo

```
$ VDC-1 %$ %POAP-2-POAP_INFO:   - Abort Power On Auto Provisioning
[yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning]
(yes/skip/no)[no]: y
Disabling POAP.....Disabling POAP
2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please
wait... (This may take 5-15 minutes)

----- System Admin Account Setup -----

Do you want to enforce secure password standard (yes/no) [y]:
```

5. Escriba **y** para aplicar el estándar de contraseña segura:

```
Do you want to enforce secure password standard (yes/no) [y]: y
```

6. Introduzca y confirme la contraseña para el administrador del usuario:

```
Enter the password for "admin":
Confirm the password for "admin":
```

7. Escriba **yes** para abrir el cuadro de diálogo Configuración básica del sistema.

Muestra el ejemplo

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco Nexus9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus9000 devices must be registered to receive entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):

8. Cree otra cuenta de inicio de sesión:

```
Create another login account (yes/no) [n]:
```

9. Configure las cadenas de comunidad SNMP de solo lectura y de lectura y escritura:

```
Configure read-only SNMP community string (yes/no) [n]:
```

```
Configure read-write SNMP community string (yes/no) [n]:
```

10. Configure el nombre del switch del clúster:

```
Enter the switch name : cs2
```

11. Configure la interfaz de gestión fuera de banda:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: y
```

```
Mgmt0 IPv4 address : 172.22.133.216
```

```
Mgmt0 IPv4 netmask : 255.255.224.0
```

```
Configure the default gateway? (yes/no) [y]: y
```

```
IPv4 address of the default gateway : 172.22.128.1
```

12. Configure las opciones avanzadas de IP:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Configurar servicios Telnet:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Configure los servicios SSH y las claves SSH:

```
Enable the ssh service? (yes/no) [y]: y
```

```
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
```

```
Number of rsa key bits <1024-2048> [1024]: 2048
```

15. Configurar otras opciones:

```
Configure the ntp server? (yes/no) [n]: n
```

```
Configure default interface layer (L3/L2) [L2]: L2
```

```
Configure default switchport interface state (shut/noshut) [noshut]:  
noshut
```

```
Configure CoPP system profile (strict/moderate/lenient/dense)  
[strict]: strict
```

16. Confirme la información del switch y guarde la configuración:

```
Would you like to edit the configuration? (yes/no) [n]: n
```

```
Use this configuration and save it? (yes/no) [y]: y
```

```
[ ] 100%
```

```
Copy complete, now saving to disk (please wait)...
```

```
Copy complete.
```

El futuro

"[Prepárese para instalar el software NX-OS y RCF](#)".

Preparar la instalación del software NX-OS y del archivo de configuración de referencia (RCF)

Antes de instalar el software NX-OS y el archivo de configuración de referencia (RCF), siga este procedimiento.

Antes de empezar

Asegúrese de tener lo siguiente:

- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- Guías de software y actualización adecuadas, disponibles en "[Switches Cisco Nexus serie 9000](#)".

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan dos nodos. Estos nodos utilizan dos puertos de interconexión de

clúster de 10 GbE e0a y.. e0b. Consulte "[Hardware Universe](#)" para verificar los puertos de clúster correctos en sus plataformas.

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches Cisco son `cs1` y.. `cs2`.
- Los nombres de nodo son `node1` y.. `node2`.
- Los nombres de LIF del clúster son `node1_clus1` y.. `node1_clus2` para los nodos 1 y `node2_clus1` y.. `node2_clus2` para el 2.
- La `cluster1::*>` prompt indica el nombre del clúster.

Acerca de esta tarea

Para ello, es necesario utilizar tanto comandos de la ONTAP como comandos de la serie Cisco Nexus 9000; los comandos de la ONTAP se usan a menos que se indique lo contrario. Los resultados del comando pueden variar en función de las diferentes versiones de ONTAP.

Pasos

1. Cambie el nivel de privilegio a avanzado, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (*>) aparece.

2. Si se habilita AutoSupport en este clúster, elimine la creación automática de casos invocando un mensaje de AutoSupport:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

donde x es la duración de la ventana de mantenimiento en horas.



El mensaje de AutoSupport notifica al soporte técnico de esta tarea de mantenimiento para que la creación automática de casos se suprima durante la ventana de mantenimiento.

El siguiente comando suprime la creación automática de casos durante dos horas:

```
cluster1:> **system node autosupport invoke -node * -type all -message  
MAINT=2h**
```

3. Muestre cuántas interfaces de interconexión de clúster se han configurado en cada nodo para cada switch de interconexión de clúster: `network device-discovery show -protocol cdp`

Muestra el ejemplo

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ 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
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

4 entries were displayed.

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. Verifique que el comando de reversión automática esté habilitado en todas las LIF de clúster:

```
network interface show -vserver Cluster -fields auto-revert
```


Muestra el ejemplo

```
cluster1::*> network interface show -vserver Cluster -fields auto-revert
```

Vserver	Logical Interface	Auto-revert
Cluster	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

```
4 entries were displayed.
```

El futuro

"[Instale el software NX-OS](#)".

Instale el software NX-OS

Siga este procedimiento para instalar el software NX-OS en el switch Nexus 92300YC.

NX-OS es un sistema operativo de red para la serie Nexus de switches Ethernet y la serie MDS de switches de red de área de almacenamiento Fibre Channel (FC) proporcionados por Cisco Systems.

Revise los requisitos

Puertos y conexiones de nodo compatibles

- Los enlaces Inter-Switch (ISL) compatibles con los switches Nexus 92300YC son los puertos 1/65 y 1/66.
- Las conexiones de nodos compatibles con los switches Nexus 92300YC son los puertos 1/1 a 1/66.

Antes de empezar

Asegúrese de tener lo siguiente:

- Software Cisco NX-OS de NetApp aplicable para sus switches desde el sitio de soporte de NetApp, disponible en "mysupport.netapp.com".
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- "[Página del switch Cisco Ethernet](#)". Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.

Instale el software

Los ejemplos de este procedimiento utilizan dos nodos, pero puede tener hasta 24 nodos en un clúster.

Acerca de los ejemplos

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de switch Nexus 92300YC son `cs1` y.. `cs2`.
- El ejemplo utilizado en este procedimiento inicia la actualización en el segundo interruptor, `*cs2*`.
- Los nombres de LIF del clúster son `node1_clus1` y.. `node1_clus2` para los nodos 1, y. `node2_clus1` y.. `node2_clus2` para el 2.
- El nombre del espacio IP es `Cluster`.
- La `cluster1::*>` prompt indica el nombre del clúster.
- Los puertos del clúster de cada nodo se llaman `e0a` y.. `e0b`.

Consulte "[Hardware Universe](#)" para los puertos de clúster reales compatibles con la plataforma.

Pasos

1. Conecte el switch de clúster a la red de gestión.
2. Utilice la `ping` Comando para verificar la conectividad con el servidor que aloja el software NX-OS y el RCF.

Muestra el ejemplo

Este ejemplo verifica que el switch puede llegar al servidor en la dirección IP 172.19.2.1:

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:

Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Copie las imágenes del software NX-OS y EPLD en el switch Nexus 92300YC.

Muestra el ejemplo

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.2.2.bin /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.2.2.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.2.2.img /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Compruebe la versión que se está ejecutando del software NX-OS:

```
show version
```

Muestra el ejemplo

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 05.31
  NXOS: version 9.2(1)
  BIOS compile time: 05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time: 7/17/2018 16:00:00 [07/18/2018 00:21:19]

Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

  Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
System version: 9.2(1)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

5. Instale la imagen NX-OS.

La instalación del archivo de imagen hace que se cargue cada vez que se reinicia el conmutador.

Muestra el ejemplo

```
cs2# install all nxos bootflash:nxos.9.2.2.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

```
Verifying image type.  
[] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.2.2.bin.  
[] 100% -- SUCCESS
```

```
Performing module support checks.  
[] 100% -- SUCCESS
```

```
Notifying services about system upgrade.  
[] 100% -- SUCCESS
```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

Images will be upgraded according to following table:

Module	Image	Running-Version(pri:alt	New-
Version	Upg-Required		
1	nxos	9.2(1)	
9.2(2)	yes		
1	bios	v05.31(05/17/2018):v05.28(01/18/2018)	
v05.33(09/08/2018)	yes		

```
Switch will be reloaded for disruptive upgrade.  
Do you want to continue with the installation (y/n)? [n] y
```

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[ ] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[ ] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[ ] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[ ] 100% -- SUCCESS
```

```
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:  
Successfully deactivated virtual service 'guestshell+'
```

```
Finishing the upgrade, switch will reboot in 10 seconds.
```

6. Compruebe la nueva versión del software NX-OS una vez que se haya reiniciado el switch:

```
show version
```

Muestra el ejemplo

```
cs2# show version
```

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
```

Software

```
BIOS: version 05.33
NXOS: version 9.2(2)
BIOS compile time: 09/08/2018
NXOS image file is: bootflash:///nxos.9.2.2.bin
NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

```
cisco Nexus9000 C92300YC Chassis
Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
Processor Board ID FDO220329V5

Device name: cs2
bootflash: 115805356 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)
```

```
Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```


Reason: Reset due to upgrade

System version: 9.2(1)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

7. Actualice la imagen de EPLD y reinicie el switch.

Muestra el ejemplo

```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.2.2.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	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.

Consulte el artículo de la base de conocimientos ["Cómo borrar la configuración en un switch de interconexión de Cisco manteniendo la conectividad remota"](#) para obtener más información al instalar o actualizar su RCF.

Acerca de esta tarea

Los ejemplos de este procedimiento utilizan la nomenclatura de conmutador y nodo siguiente:

- Los nombres de los dos switches Cisco son `cs1` y.. `cs2`.
- Los nombres de nodo son `node1` y.. `node2`.
- Los nombres de LIF del clúster son `node1_clus1`, `node1_clus2`, `node2_clus1`, y. `node2_clus2`.
- La `cluster1::*>` prompt indica el nombre del clúster.



- El procedimiento requiere el uso de tanto comandos de la ONTAP como de ["Switches Cisco Nexus serie 9000"](#); Los comandos ONTAP se utilizan a menos que se indique lo contrario.
- Antes de realizar este procedimiento, asegúrese de que tiene una copia de seguridad actual de la configuración del conmutador.
- Durante este procedimiento no se necesita ningún enlace entre switches (ISL) operativo. Esto se debe a que los cambios en la versión de RCF pueden afectar temporalmente a la conectividad ISL. Para garantizar operaciones de clúster no disruptivas, el siguiente procedimiento migra todas las LIF del clúster al switch de partner operativo mientras realiza los pasos del switch de destino.

Pasos

1. Muestre los puertos del clúster en cada nodo que están conectados a los switches de clúster:

```
network device-discovery show
```

Muestra el ejemplo

```
cluster1::*> *network device-discovery show*
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1/cdp
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 -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
-----
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*

Current      Logical      Status      Network
Vserver      Current Is
Port         Interface   Admin/Oper  Address/Mask  Node
-----
Cluster
e0c          node1_clus1  up/up      169.254.3.4/23  node1
e0d          node1_clus2  up/up      169.254.3.5/23  node1
e0c          node2_clus1  up/up      169.254.3.8/23  node2
e0d          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. Vuelva a aplicar las personalizaciones anteriores a la configuración del conmutador. Consulte la ["Revise las consideraciones sobre el cableado y la configuración"](#) para obtener información detallada sobre cualquier cambio adicional necesario.
3. Después de comprobar que las versiones de RCF y los ajustes del switch son correctos, copie el archivo running-config en el archivo startup-config.

Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Switches Cisco Nexus serie 9000"](#) guías.

```
cs2# copy running-config startup-config  
[] 100% Copy complete
```

4. Reinicie el interruptor cs2. Es posible ignorar los eventos "puertos de clúster inactivos" que se informan en los nodos mientras se reinicia el switch.

```
cs2# reload  
This command will reboot the system. (y/n)? [n] y
```

5. Compruebe el estado de los puertos del clúster en el clúster.
 - a. Compruebe que los puertos e0d están en buen estado y en todos los nodos del clúster:

```
network port show -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



```

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.
```

6. En el switch de clúster cs1, apague los puertos conectados a los puertos del clúster de los nodos.

En el ejemplo siguiente se utiliza el resultado del ejemplo de interfaz del paso 1:

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

7. Comprobar que las LIF del clúster han migrado a los puertos alojados en el switch cs2. Esto puede tardar unos segundos. `network interface show -vserver Cluster`

Muestra el ejemplo

```
cluster1::*> *network interface show -vserver Cluster*
      Logical      Status      Network      Current
Current Is
Vserver  Interface    Admin/Oper Address/Mask  Node
Port    Home
-----
Cluster
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::*>
```

8. Compruebe que el clúster esté en buen estado:

```
cluster show
```


Muestra el ejemplo

```
cluster1::*> *cluster show*
Node           Health   Eligibility   Epsilon
-----
node1          true    true         false
node2          true    true         false
cluster1::*>
```

9. Repita los pasos 7 a 14 en el interruptor cs1.
10. Habilite la reversión automática en las LIF del clúster.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert True
```

11. Reinicie el interruptor cs1. Para activar las LIF de clúster y revertir a sus puertos raíz, haga lo siguiente. Es posible ignorar los eventos "puertos de clúster inactivos" que se informan en los nodos mientras se reinicia el switch.

```
cs1# reload
This command will reboot the system. (y/n)? [n] y
```

12. Compruebe que los puertos del switch conectados a los puertos del clúster estén activos.

```
cs1# show interface brief | grep up
.
.
Ethernet1/1      1      eth  access up    none
10G(D) --
Ethernet1/2      1      eth  access up    none
10G(D) --
Ethernet1/3      1      eth  trunk  up    none
100G(D) --
Ethernet1/4      1      eth  trunk  up    none
100G(D) --
.
.
```

13. Compruebe que el ISL entre cs1 y cs2 funciona:
show port-channel summary

Muestra el ejemplo

```
cs1# *show port-channel summary*
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)      Eth       LACP      Eth1/65 (P)  Eth1/66 (P)
cs1#
```

14. Compruebe que las LIF del clúster han vuelto a su puerto de inicio:

network interface show -vserver Cluster

Muestra el ejemplo

```
cluster1::*> *network interface show -vserver Cluster*

          Logical      Status      Network      Current
Current Is
Vserver   Interface    Admin/Oper  Address/Mask  Node
Port      Home
-----
-----
Cluster
          node1_clus1  up/up      169.254.3.4/23  node1
e0d       true
          node1_clus2  up/up      169.254.3.5/23  node1
e0d       true
          node2_clus1  up/up      169.254.3.8/23  node2
e0d       true
          node2_clus2  up/up      169.254.3.9/23  node2
e0d       true
cluster1::*>
```

15. Compruebe que el clúster esté en buen estado:

```
cluster show
```

Muestra el ejemplo

```
cluster1::*> *cluster show*
Node           Health Eligibility Epsilon
-----
node1           true   true     false
node2           true   true     false
```

16. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination					
Packet		LIF		LIF					
Node	Date								
Loss									

node1									
	3/5/2022 19:21:18 -06:00	node1_clus2		node2-clus1					
node									
	3/5/2022 19:21:20 -06:00	node1_clus2		node2_clus2					
node									
node2									
	3/5/2022 19:21:18 -06:00	node2_clus2		node1_clus1					
node									
	3/5/2022 19:21:20 -06:00	node2_clus2		node1_clus2					
node									

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)

```

El futuro

["Compruebe la configuración de SSH".](#)

Compruebe su configuración SSH

Si utiliza la supervisión de estado del switch Ethernet (CSHM) y las funciones de recogida de registros, compruebe que las claves SSH y SSH estén habilitadas en los switches de clústeres.

Pasos

1. Compruebe que SSH está habilitado:

```
(switch) show ssh server  
ssh version 2 is enabled
```

2. Compruebe que las claves SSH estén habilitadas:

```
show ssh key
```

Muestra el ejemplo

```
(switch)# show ssh key  
  
rsa Keys generated:Fri Jun 28 02:16:00 2024  
  
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQgQDiNrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew  
17nwlIoc6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yIPTBoIZZxbWRShywAM5  
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==  
  
bitcount:1024  
fingerprint:  
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo  
  
could not retrieve dsa key information  
  
ecdsa Keys generated:Fri Jun 28 02:30:56 2024  
  
ecdsa-sha2-nistp521  
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e  
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z  
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVliewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1  
u/9Pzh/Vz9cHDcCW9qGE780QHA==  
  
bitcount:521  
fingerprint:  
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRALZeHwQ  
  
(switch)# show feature | include scpServer  
scpServer          1          enabled  
(switch)# show feature | include ssh  
sshServer          1          enabled  
(switch)#
```



Al habilitar FIPS, debe cambiar el bitcount a 256 en el conmutador mediante el comando `ssh key ecdsa 256 force`. Consulte ["Configurar la seguridad de red con FIPS"](#) para obtener más información.

El futuro

["Configure la supervisión de estado del switch"](#).

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 completada 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. Ver ["Monitoreo del estado del conmutador \(CSHM\)"](#).

Revise los requisitos

Antes de empezar

Asegúrese de tener lo siguiente:

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
-mmessage 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
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: 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
cs1 (FDO220329KU) Eth1/65	Eth1/65	177	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	177	R S I s	N9K-C92300YC

Total entries displayed: 2

4. Compruebe que todos los puertos del clúster estén activos:

```
network port show -ip space 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					
	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.

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					
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
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 la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local

Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)
```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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
```

2. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

El futuro

"Configure la supervisión de estado del switch".

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 completada 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. Ver ["Monitoreo del estado del conmutador \(CSHM\)"](#).

Revise los requisitos

Antes de empezar

Asegúrese de tener lo siguiente:

- 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 la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

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
C92300YC			N9K-
	e0b	cs2	0/2
C92300YC			N9K-
node1	/cdp		
	e0a	cs1	0/1
C92300YC			N9K-
	e0b	cs2	0/1
C92300YC			N9K-

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 la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e0a
Cluster node1_clus2 169.254.49.125 node1      e0b
Cluster node2_clus1 169.254.47.194 node2      e0a
Cluster node2_clus2 169.254.19.183 node2      e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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

```

2. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```

El futuro

"Configure la supervisión de estado del switch".

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

Antes de empezar

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.

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después de las tareas de mantenimiento para deshabilitar la creación de casos durante el mantenimiento. Consulte este artículo de la base de conocimientos ["SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#) para obtener más detalles.
- Habilite el registro de sesiones para cualquier sesión de CLI. Para obtener instrucciones sobre cómo activar el registro de sesiones, consulte la sección «Salida de sesión de registro» de este artículo de la base de conocimientos ["Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP"](#).

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 la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
-----	-----				
e0a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e0b	Cluster	Cluster		up	9000
healthy	false				auto/10000

```
Node: node2
```

```
Ignore
```

Health	Health				Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status				Admin/Oper
-----	-----	-----	-----	-----	-----
-----	-----				
e0a	Cluster	Cluster		up	9000
healthy	false				auto/10000
e0b	Cluster	Cluster		up	9000
healthy	false				auto/10000

```
4 entries were displayed.
```

Paso 3: Complete el procedimiento

1. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source		Destination	
Packet					
Node	Date		LIF		LIF
Loss					
-----	-----	-----	-----	-----	-----
node1					
	3/5/2022 19:21:18 -06:00		node1_clus2		node2-clus1
node					
	3/5/2022 19:21:20 -06:00		node1_clus2		node2_clus2
node					
node2					
	3/5/2022 19:21:18 -06:00		node2_clus2		node1_clus1
node					
	3/5/2022 19:21:20 -06:00		node2_clus2		node1_clus2
node					

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)
```

1. Confirme la siguiente configuración de red de cluster:

```
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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
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

El futuro

["Configure la supervisión de estado del switch".](#)

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.

Antes de empezar

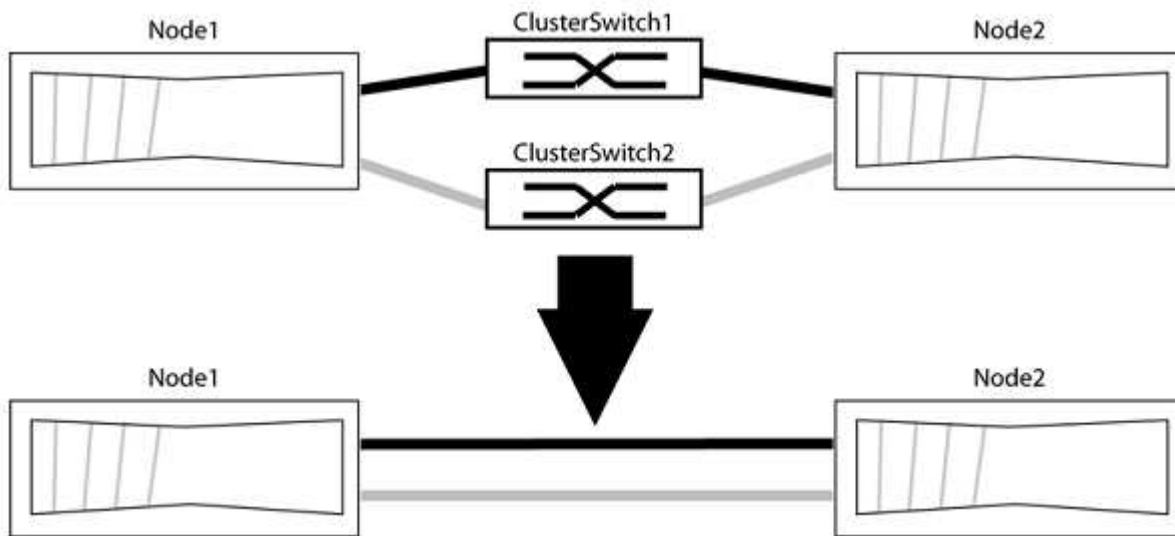
Asegúrese de tener lo siguiente:

- 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

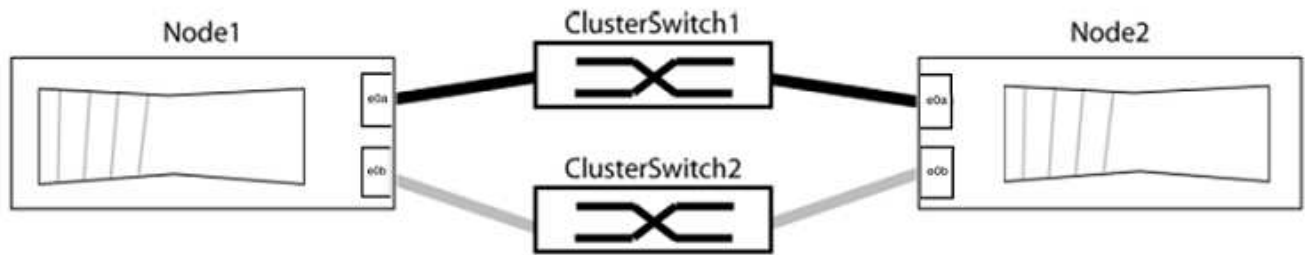
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

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 de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source	Destination
Packet			
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node1			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node2			

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Verifique que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

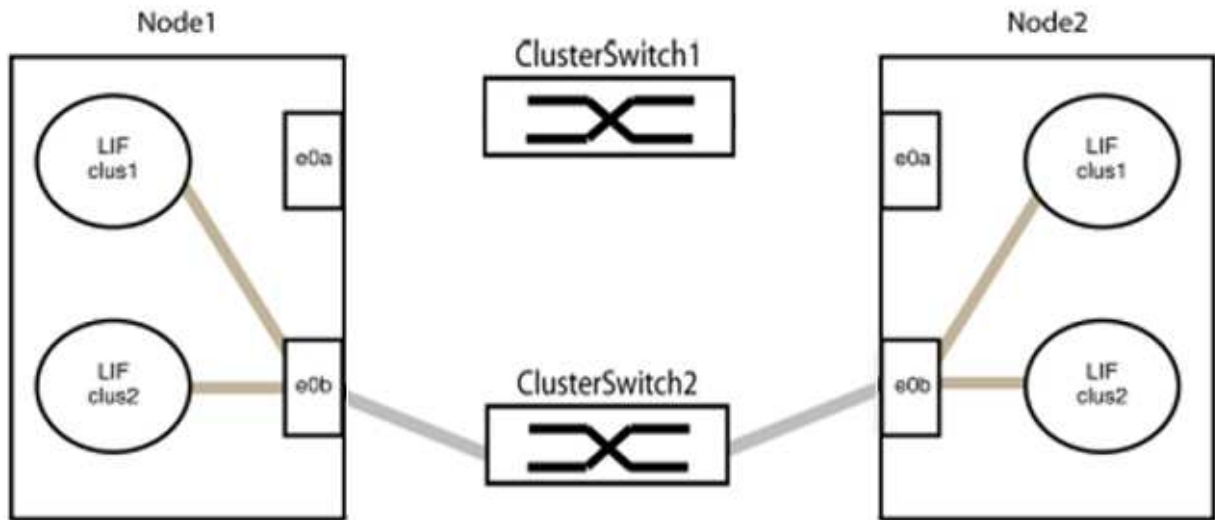
2. Configure la configuración sin switches para los puertos del grupo 1.



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**.

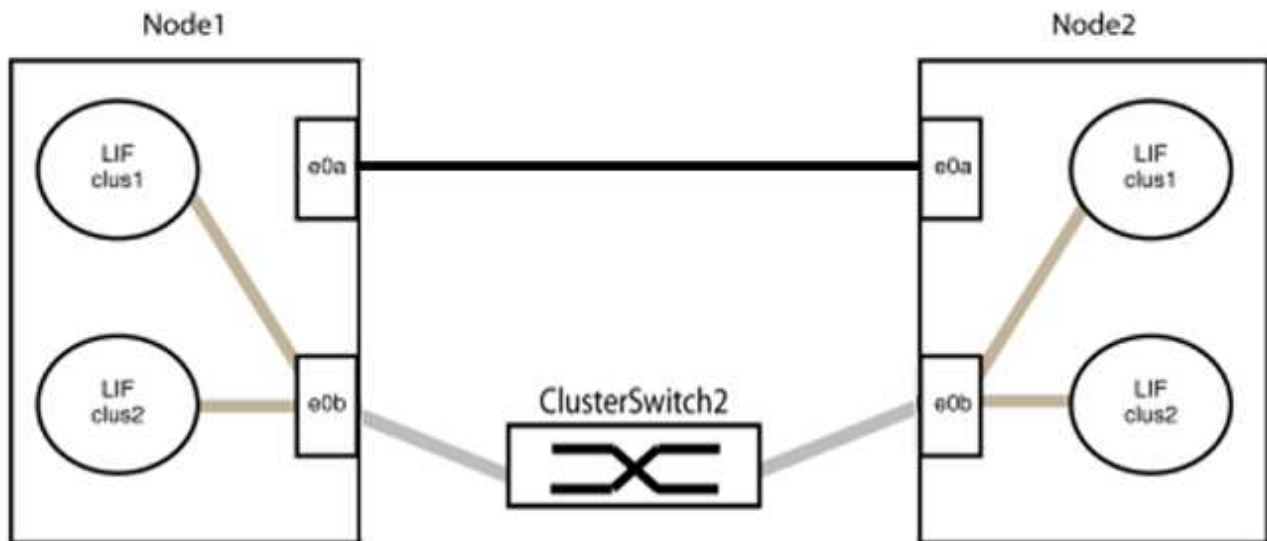
- a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

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:



3. 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
```

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			

node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node			

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)
```



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.

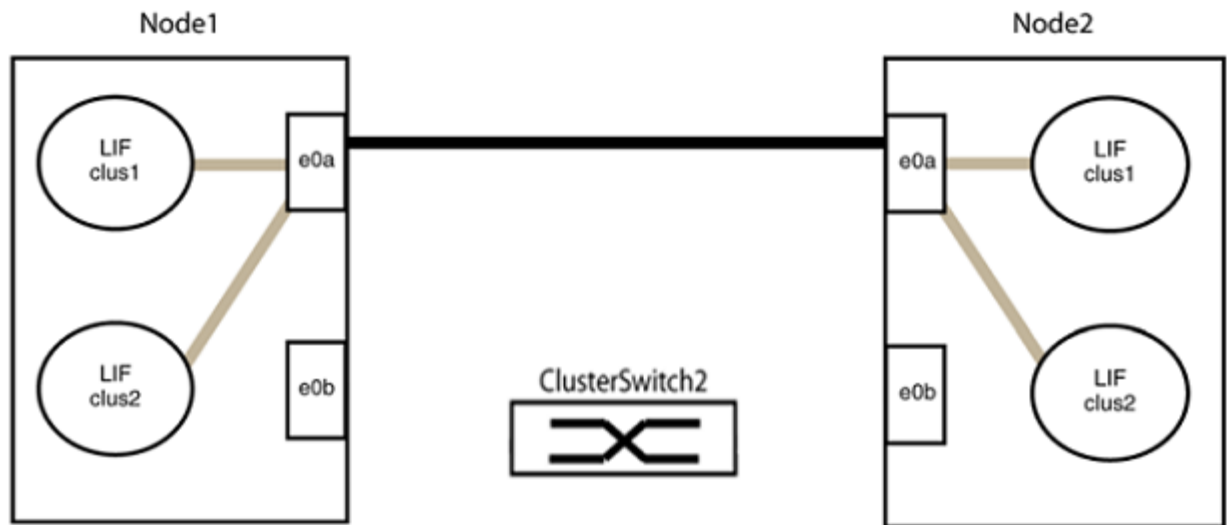
1. Configure la configuración sin switch para los puertos del grupo 2.



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**.

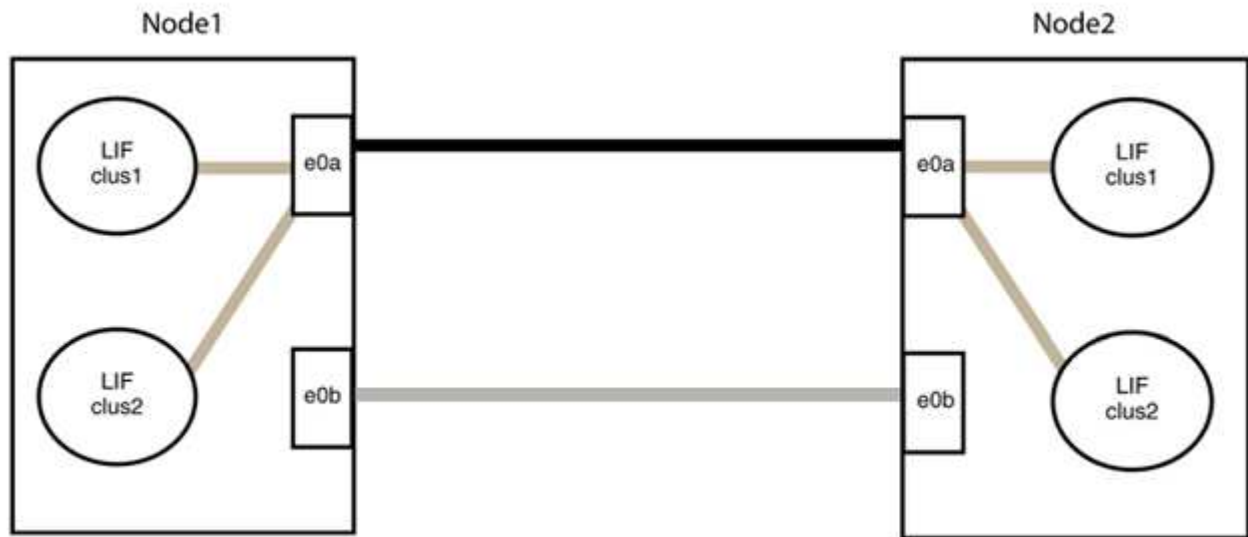
- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

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 épsilon en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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"](#).

2. 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.
"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	Proporciona ejemplos de cómo utilizar el switch CN1601 en una red típica. • "Guía del administrador" • "Guía del administrador, Versión 1.1.x.x" • "Guía del administrador, Versión 1.2.x.x"

Título del documento	Descripción
Referencia de comandos de CLI del switch de red CN1610	Proporciona información detallada acerca de los comandos de la interfaz de línea de comandos (CLI) que utiliza para configurar el software CN1601. • "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

Antes de empezar

Asegúrese de tener lo siguiente:

- 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 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.

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

Antes de empezar

Asegúrese de tener lo siguiente:

- 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 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.
- 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
```

					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

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.

El futuro

["Configure la supervisión de estado del switch"](#)

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

Antes de empezar

Asegúrese de tener lo siguiente:

- 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
```

(Mbps)						Speed
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

Antes de empezar

Asegúrese de tener lo siguiente:

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.

El ["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"](#)
- ["NetApp CN1601 y CN1610"](#)
- ["Configuración y configuración de los conmutadores 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.

El "[Hardware Universe](#)" Contiene la información más reciente sobre los puertos de clúster reales para sus 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/	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		

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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

		Source	Destination
Packet			
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Migrar clus1 al puerto E2A en 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`

2. 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
```

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	e2a
false					
	clus2	up/up	10.10.10.2/16	node1	e2a
true					
node2					
	clus1	up/up	10.10.11.1/16	node2	e2a
false					
	clus2	up/up	10.10.11.2/16	node2	e2a
true					

4 entries were displayed.

3. 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
```

4. 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
```

9. 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.

10. 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>>`

11. 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.
```

12. 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
```

13. 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`

14. 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.

15. 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
```

16. 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.

17. 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.
18. 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.
19. 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
```

20. 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
```

21. 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.

22. 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. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node2		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2
node		

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Verifique que ambos nodos tengan 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
```

2. Muestra información sobre los dispositivos de la configuración:

```
network device discovery show
```

3. 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.

4. 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.

5. 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.

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:

```
cluster::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true    true         false
node2                true    true         false
```

7. 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
```

8. 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).

Revise los requisitos

Antes de empezar

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.

Active el registro de la consola

NetApp recomienda encarecidamente que habilite el inicio de sesión de la consola en los dispositivos que esté utilizando y que realice las siguientes acciones al sustituir el conmutador:

- Deje la función AutoSupport habilitada durante el mantenimiento.
- Active un AutoSupport de mantenimiento antes y después de las tareas de mantenimiento para deshabilitar la creación de casos durante el mantenimiento. Consulte este artículo de la base de conocimientos ["SU92: Cómo impedir la creación automática de casos durante las ventanas de mantenimiento programado"](#) para obtener más detalles.
- Habilite el registro de sesiones para cualquier sesión de CLI. Para obtener instrucciones sobre cómo activar el registro de sesiones, consulte la sección «Salida de sesión de registro» de este artículo de la base de conocimientos ["Cómo configurar PuTTY para una conectividad óptima con sistemas ONTAP"](#).

Sustituya el interruptor

Acercas 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 "IOIO" 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

```
(new_cs1)# config
(new_cs1)(config)# interface 0/1-0/12
(new_cs1)(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.

Antes de empezar

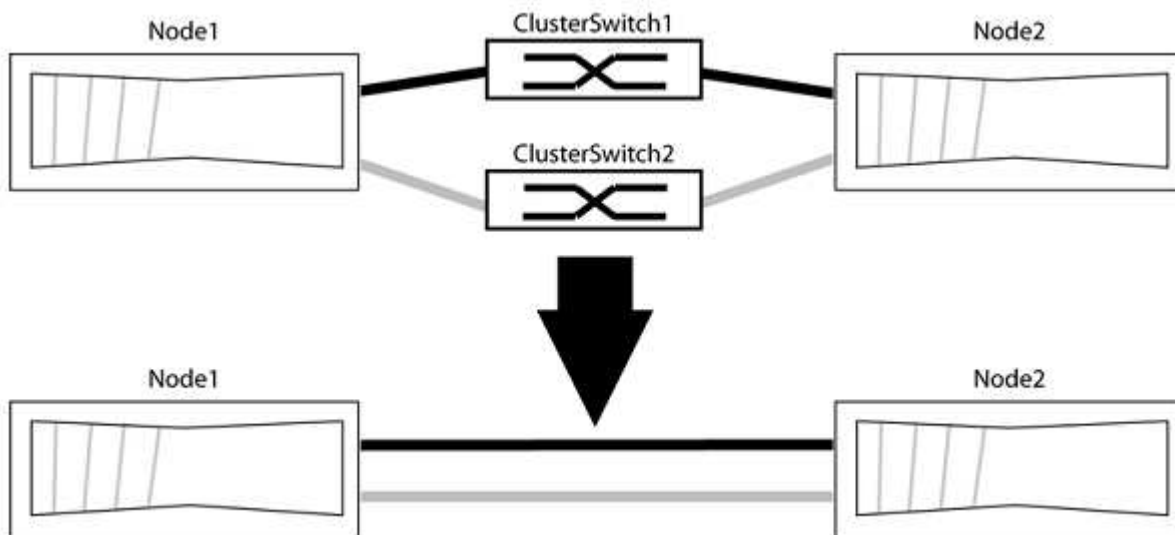
Asegúrese de tener lo siguiente:

- 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

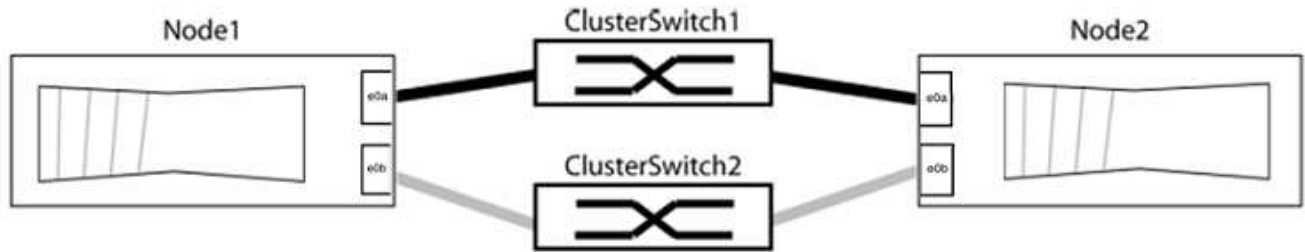
```
cluster::*> system node autosupport invoke -node * -type all
-messsage MAINT=2h
```

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 de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Verifique que el clúster esté en buen estado:

```
cluster ring show
```

Todas las unidades deben ser maestra o secundaria.

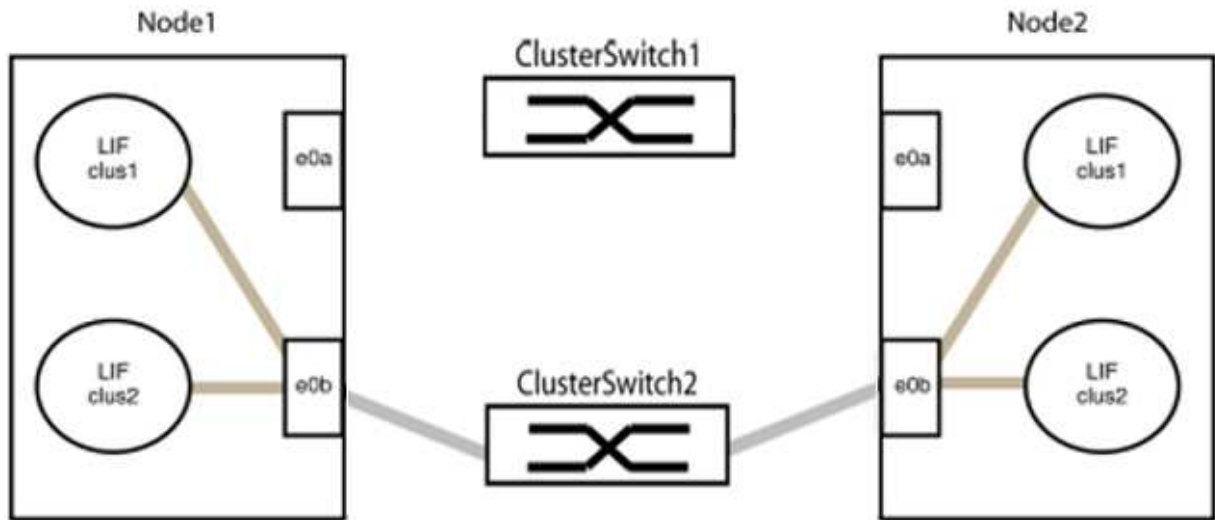
2. Configure la configuración sin switches para los puertos del grupo 1.



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**.

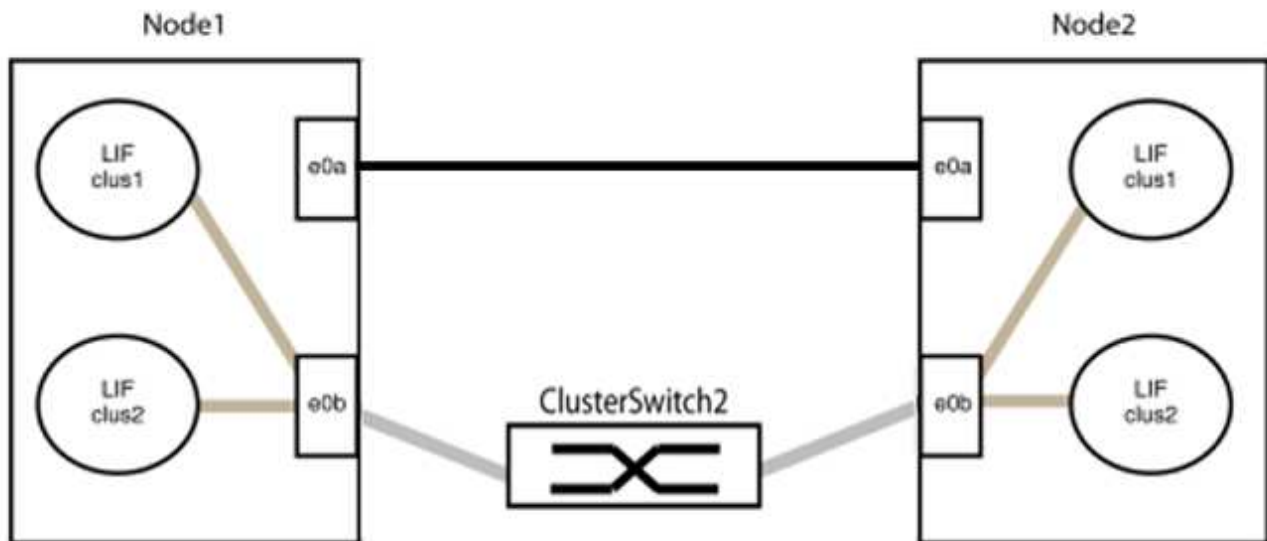
- a. Desconecte todos los cables de los puertos del grupo 1 al mismo tiempo.

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:



3. 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
```

4. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet	Source	Destination
Node	LIF	LIF
Date		
Loss		
-----	-----	-----
node1		
3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2		
3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1		
3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2		
3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```



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.

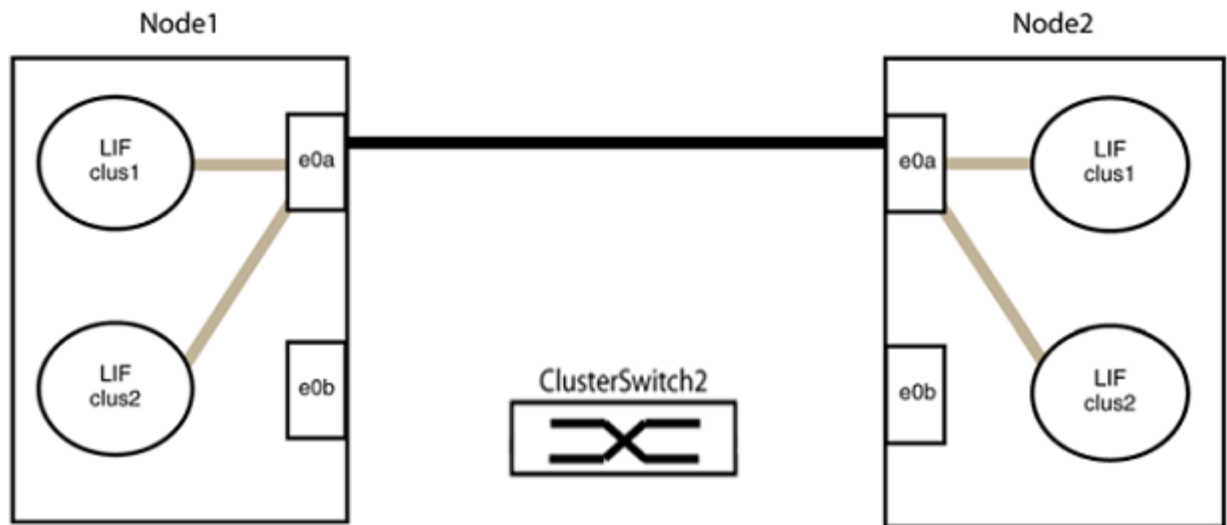
1. Configure la configuración sin switch para los puertos del grupo 2.



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**.

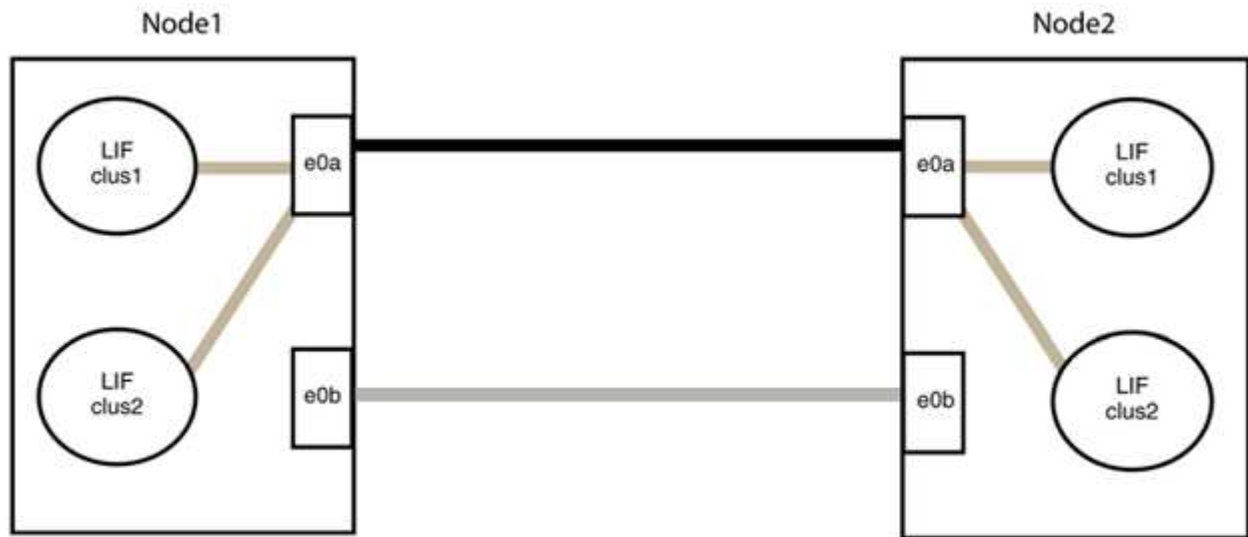
- a. Desconecte todos los cables de los puertos del grupo 2 al mismo tiempo.

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 épsilon en ambos nodos que desee false:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Compruebe la conectividad de las interfaces del clúster remoto:

ONTAP 9.9.1 y versiones posteriores

Puede utilizar el `network interface check cluster-connectivity` comando para iniciar una comprobación de accesibilidad de la conectividad del clúster y, a continuación, muestre los detalles:

```
network interface check cluster-connectivity start y..network interface check cluster-connectivity show
```

```
cluster1::*> network interface check cluster-connectivity start
```

NOTA: Espere varios segundos antes de ejecutar el `show` comando para mostrar los detalles.

```
cluster1::*> network interface check cluster-connectivity show
```

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----	-----	-----	-----
node1			
	3/5/2022 19:21:18 -06:00	node1_clus2	node2-clus1
node2			
	3/5/2022 19:21:20 -06:00	node1_clus2	node2_clus2
node1			
	3/5/2022 19:21:18 -06:00	node2_clus2	node1_clus1
node2			
	3/5/2022 19:21:20 -06:00	node2_clus2	node1_clus2

Todos los lanzamientos de ONTAP

En todas las versiones de ONTAP, también se puede utilizar el `cluster ping-cluster -node <name>` comando para comprobar la conectividad:

```
cluster ping-cluster -node <name>
```

```

cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 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)

```

1. Si suprimió la creación automática de casos, vuelva a activarlo 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"](#).

2. Vuelva a cambiar el nivel de privilegio a admin:

```
set -privilege admin
```


Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de privacidad

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.