



Cisco Nexus 9336C-FX2

Cluster and storage switches

NetApp
April 25, 2024

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems-switches/switch-cisco-9336c-fx2-storage/configure-switch-overview-9336c-storage.html> on April 25, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Cisco Nexus 9336C-FX2 1
 - Descripción general 1
 - Instale el hardware 5
 - Configurar el software 12
 - Sustituya un switch de almacenamiento Cisco Nexus 9336C-FX2 65

Cisco Nexus 9336C-FX2

Descripción general

Descripción general de la instalación y la configuración de los switches de almacenamiento Cisco Nexus 9336C-FX2

El switch de almacenamiento Cisco Nexus 9336C-FX2 forma parte de la plataforma Cisco Nexus 9000 y se puede instalar en un armario rack de sistemas de NetApp. Los switches de almacenamiento le permiten enrutar datos entre servidores y matrices de almacenamiento en una red DE área de almacenamiento (SAN).

Información general de configuración inicial

Para configurar un switch Cisco Nexus 9336C-FX2 en sistemas que ejecutan ONTAP, siga estos pasos:

1. ["Complete la hoja de cálculo de cableado"](#).
2. ["Instale el interruptor"](#).
3. ["Configurar el switch"](#).
4. ["Instale el switch en el armario de NetApp"](#).

En función de la configuración, podrá instalar el switch y el panel de paso a través de Cisco Nexus 9336C-FX2 en un armario de NetApp con los soportes estándar que se incluyen con el switch.

5. ["Prepare la instalación de NX-OS y RCF"](#).
6. ["Instale el software NX-OS"](#).
7. ["Instale el archivo de configuración RCF"](#).

Instale el RCF después de configurar por primera vez el conmutador Nexus 9336C-FX2. También puede utilizar este procedimiento para actualizar la versión de RCF.

Información adicional

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

- ["Requisitos de configuración"](#)
- ["Componentes y números de pieza"](#)
- ["Documentación requerida"](#)
- ["Requisitos de Smart Call Home"](#)

Requisitos de configuración de los switches de almacenamiento 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"](#).

Los componentes y números de pieza de los switches de almacenamiento 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
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT10/25/40/100GQSFP28
X190002	Kit de accesorios X190001/X190003

Número de pieza	Descripción
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

Requisitos de documentación de los switches de almacenamiento 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.

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.

Título del documento	Descripción
<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 (elija las notas para la versión de NX-OS instalada en los switches)</i>	Describe las funciones, errores y limitaciones de Cisco Nexus 9000 Series.
Cumplimiento normativo e información de seguridad para Cisco Nexus serie 9000	Proporciona información legal, de seguridad y cumplimiento de normativas de agencias internacionales para los switches de la serie Nexus 9000.

Documentación de los sistemas ONTAP

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

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

Kit de raíl y documentación del armario

Para instalar un switch Cisco 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 la función de inicio de llamada inteligente, revise las siguientes directrices.

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

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

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

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

Instale el hardware

Instale el switch de almacenamiento 9336C-FX2

Siga este procedimiento para instalar el switch de almacenamiento Cisco Nexus 9336C-FX2.

Lo que necesitará

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

Si está instalando el...	Realice lo siguiente...
Equipo en un bastidor de Telco	Consulte los procedimientos proporcionados en las guías de instalación del hardware del switch y las instrucciones de instalación y configuración de NetApp.

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

Vaya a. ["Configurar el switch de almacenamiento Cisco Nexus 9336C-FX2"](#).

Configurar el switch de almacenamiento 9336C-FX2

Siga este procedimiento para configurar el switch Cisco Nexus 9336C-FX2.

Lo que necesitará


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

Prompt	Respuesta
¿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
¿Servicio SSH habilitado? (sí/no)	<p>Responda con sí. El valor predeterminado es yes.</p> <div>  <p>Se recomienda SSH cuando se utilice el Monitor de estado del conmutador de clúster (CSHM) para sus funciones de recopilación de registros. También se recomienda SSHv2 para mejorar la seguridad.</p> </div>
Introduzca el tipo de clave SSH que desea generar (dsa/rsa/rsa1).	El valor predeterminado es rsa .
Introduzca el número de bits de clave (1024-2048).	Introduzca el número de bits de clave de 1024 a 2048.
¿Configurar el servidor NTP? (sí/no)	Responda con no . El valor predeterminado es no

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

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

El futuro

Opcionalmente, puede hacerlo ["Instale un switch Cisco Nexus 9336C-FX2 en un armario de NetApp"](#). De lo contrario, vaya a ["Prepare la instalación de NX-OS y RCF"](#).

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.

Lo que necesitará

- 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.

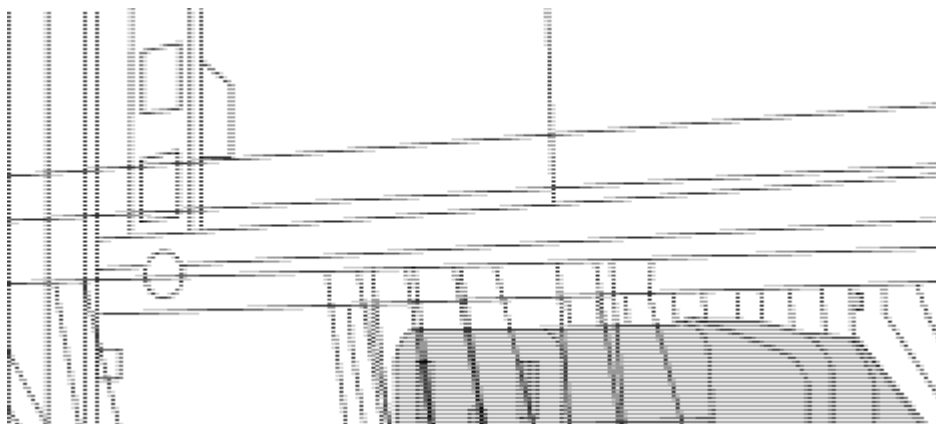
NetApp puede adquirir el kit de panel de paso a través (número de pieza X8784-R6).

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.

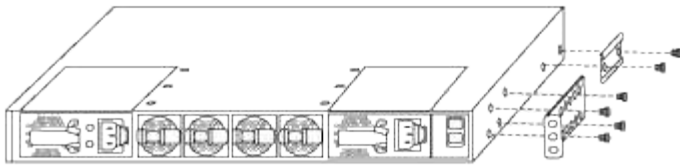
En este procedimiento, el panel de limpieza se instalará en U40.

- 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.

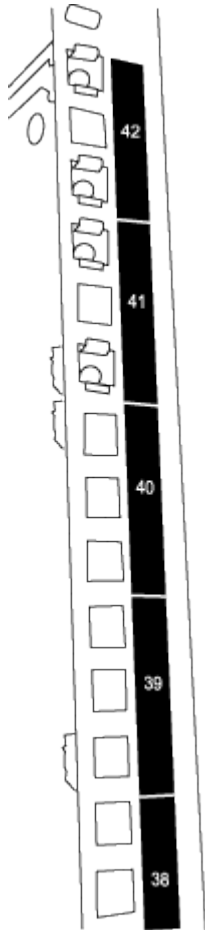


(1) conector hembra del cable puente.

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.

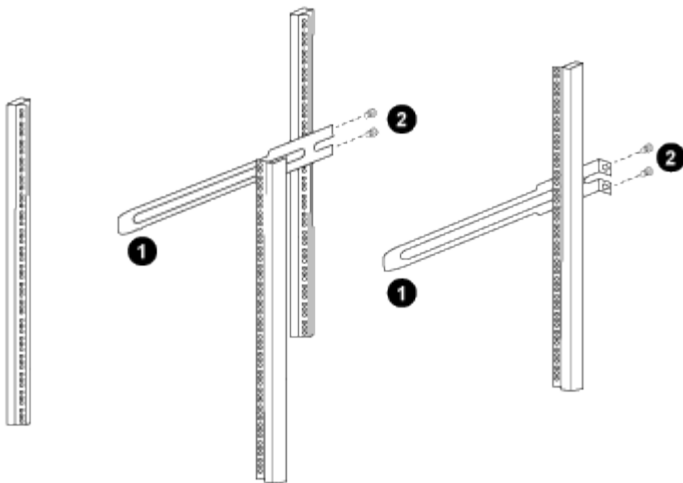


- b. Repita el paso 2 a con el otro soporte de montaje en bastidor delantero en el otro lado del interruptor.
 - c. Instale el soporte de montaje en bastidor trasero en el chasis del interruptor.
 - d. Repita el paso 2c con el otro soporte de montaje en bastidor trasero en el otro lado del interruptor.
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.

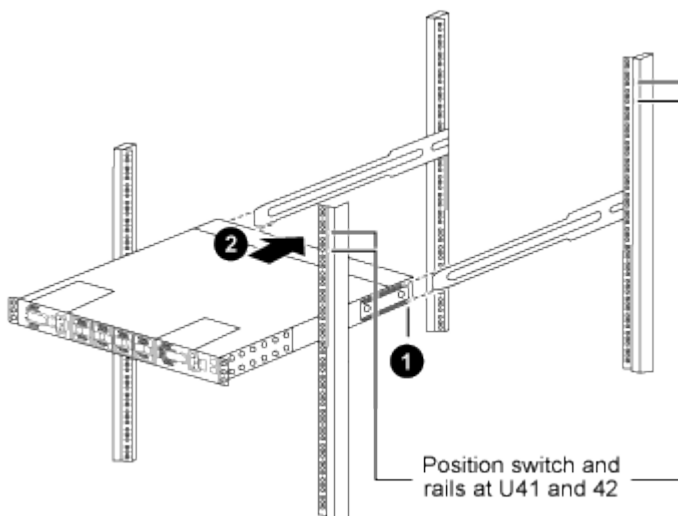
- a. Repita el paso 4a para el poste trasero derecho.
- b. Repita los pasos 4a y 4b en las ubicaciones del RU41 en el armario.

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.

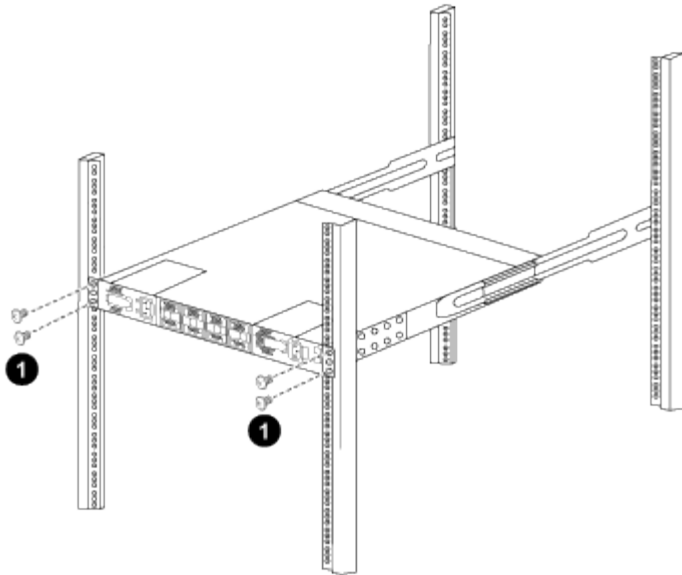
- a. Coloque la parte posterior del interruptor en RU41.



(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 por 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 los switches de almacenamiento Cisco Nexus 9336C-FX2

Para instalar y configurar el software de un switch Cisco Nexus 9336C-FX2, siga estos pasos:

1. "Prepare la instalación de NX-OS y RCF".
2. "Instale el software NX-OS".

3. "Instale el archivo de configuración RCF".

Instale el RCF después de configurar por primera vez el conmutador Nexus 9336C-FX2. También puede utilizar este procedimiento para actualizar la versión de 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 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 -ip space 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 Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.209.69/16	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.49.125/16	
cluster1-01	e0b true			
	cluster1-02_clus1	up/up	169.254.47.194/16	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.19.183/16	
cluster1-02	e0b true			
4 entries were displayed.				

5. Haga ping en las LIF de cl ster remoto:

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

Muestra el ejemplo

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

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

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

6. Compruebe que el comando de reversión automática está habilitado en todas las LIF del clúster:

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

Muestra el ejemplo

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

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

4 entries were displayed.

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

```
system switch ethernet log setup-password y.. system switch ethernet log enable-collection
```

Muestra el ejemplo

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



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

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

```
system cluster-switch log setup-password y..system cluster-switch log enable-  
collection
```

Muestra el ejemplo

```
cluster1::*> system cluster-switch log setup-password  
Enter the switch name: <return>  
The switch name entered is not recognized.  
Choose from the following list:  
cs1  
cs2  
  
cluster1::*> system cluster-switch log setup-password  
  
Enter the switch name: cs1  
RSA key fingerprint is  
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc  
Do you want to continue? {y|n}::[n] y  
  
Enter the password: <enter switch password>  
Enter the password again: <enter switch password>  
  
cluster1::*> system cluster-switch log setup-password  
  
Enter the switch name: cs2  
RSA key fingerprint is  
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1  
Do you want to continue? {y|n}:: [n] y  
  
Enter the password: <enter switch password>  
Enter the password again: <enter switch password>  
  
cluster1::*> system cluster-switch log enable-collection  
  
Do you want to enable cluster log collection for all nodes in the  
cluster?  
{y|n}: [n] y  
  
Enabling cluster switch log collection.  
  
cluster1::*>
```



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

El futuro

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

Instale el software NX-OS

Siga este procedimiento para instalar el software NX-OS en el switch de clúster Nexus 9336C-FX2.

Antes de comenzar, complete el procedimiento en ["Prepare la instalación de NX-OS y RCF"](#).

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- ["Página del switch Cisco Ethernet"](#). Consulte en la tabla de compatibilidad del switch las versiones ONTAP y NX-OS compatibles.
- Guías de software y actualización adecuadas disponibles en el sitio web de Cisco para los procedimientos de actualización y degradación de switches de Cisco. Consulte ["Switches Cisco Nexus serie 9000"](#).

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
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 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.
```

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

```
show version
```


Muestra el ejemplo

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

Software
  BIOS: version 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#
```

5. Instale la imagen NX-OS.

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

Muestra el ejemplo

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

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

```
show version
```

Muestra el ejemplo

```
cs2# show version
```

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

```
TAC support: http://www.cisco.com/tac
```

```
Copyright (C) 2002-2020, Cisco and/or its affiliates.
```

```
All rights reserved.
```

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

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

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

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

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

```
A copy of each such license is available at
```

```
http://www.opensource.org/licenses/gpl-2.0.php and
```

```
http://opensource.org/licenses/gpl-3.0.html and
```

```
http://www.opensource.org/licenses/lgpl-2.1.php and
```

```
http://www.gnu.org/licenses/old-licenses/library.txt.
```

Software

```
  BIOS: version 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):
```

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.9.3.5.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

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

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

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

Muestra el ejemplo

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

EPLD	Device	Version
MI	FPGA	0x7
IO	FPGA	0x19
MI	FPGA2	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2

9. Repita los pasos 1 a 8 para instalar el software NX-OS en el interruptor CS1.

El futuro

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

Instalación del archivo de configuración de referencia (RCF)

Puede instalar el RCF después de configurar por primera vez el conmutador Nexus 9336C-FX2. También puede utilizar este procedimiento para actualizar la versión de RCF.

Antes de comenzar, complete el procedimiento en ["Prepare la instalación de NX-OS y RCF"](#).

Revise los requisitos

Lo que necesitará

- Una copia de seguridad actual de la configuración del switch.
- Un clúster en pleno funcionamiento (sin errores en los registros o problemas similares).
- El archivo RCF actual.
- Una conexión de consola al conmutador, necesaria para instalar el RCF.

Documentación sugerida

- ["Página del switch Cisco Ethernet"](#) Consulte la tabla de compatibilidad del conmutador para conocer las versiones ONTAP y RCF admitidas. Tenga en cuenta que puede haber dependencias de comandos entre la sintaxis del comando en el RCF y la que se encuentra en las versiones de NX-OS.
- ["Switches Cisco Nexus serie 3000"](#). Consulte las guías de software y actualización adecuadas disponibles en el sitio web de Cisco para obtener documentación completa sobre los procedimientos de actualización y degradación de switches de Cisco.

Instale el RCF

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.

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.

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.

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 conmutador mediante la consola serie. Esta tarea restablece la configuración de la red de gestión.

Paso 1: Prepare la instalación

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.

Muestra el ejemplo

```
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.

Muestra el ejemplo

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

2. 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			
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. 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
```

6. Copie el RCF en el bootflash del conmutador cs2 utilizando uno de los siguientes protocolos de transferencia: FTP, TFTP, SFTP o SCP. Para obtener más información acerca de los comandos de Cisco, consulte la guía correspondiente en ["Referencia de comandos NX-OS de Cisco Nexus serie 9000"](#) 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_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)...
```

7. 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 instalación en el conmutador cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

8. 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

```
cs2# 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
*
*****
*****
```

9. 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.

10. 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 9000"](#) guías.

Muestra el ejemplo

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

11. Reinicie el interruptor cs2. Puede ignorar los eventos «cluster ports down» notificados en los nodos mientras se reinicia el switch.

Muestra el ejemplo

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

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

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

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

Muestra el ejemplo

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

Health						Speed(Mbps)	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.

- a. 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
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	Type	Address
Model		

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.

```

13. 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:

```

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

```

14. 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::*>				

15. 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::*>
```

16. Repita los pasos 4 a 11 en el interruptor CS1.
17. Habilite la reversión automática en las LIF del clúster.

Muestra el ejemplo

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

18. Reinicie el interruptor cs1. Para activar las LIF de clúster y revertir a sus puertos raíz, haga lo siguiente. Puede ignorar los eventos «cluster ports down» notificados en los nodos mientras se reinicia el switch.

Muestra el ejemplo

```
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 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          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1        133      H                FAS2980
e0a
node2              Eth1/2        133      H                FAS2980
e0a
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
```

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::*>				

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

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

Muestra el ejemplo

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

Recopilación de registro de supervisión del estado del switch Ethernet

Es posible usar la función de recopilación de registros para recoger archivos de registro relacionados con switches en ONTAP.

+

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

Antes de empezar

- Compruebe que ha configurado su entorno mediante el conmutador de clúster 9336C-FX2 **CLI**.
- La monitorización del estado del interruptor debe estar activada para el interruptor. Verifique esto asegurándose de que el `Is Monitored:` el campo se establece en **true** en la salida del `system switch ethernet show` comando.

Pasos

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

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

Muestra el ejemplo

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

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

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

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

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

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

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

2. Para iniciar la recopilación de registros, ejecute el siguiente comando, sustituyendo EL DISPOSITIVO por

el conmutador utilizado en el comando anterior. Esto inicia ambos tipos de recopilación de registros: Los registros detallados de **Support** y una recopilación horaria de datos **Periódicos**.

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

Muestra el ejemplo

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

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

Enabling cluster switch log collection.

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

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

Enabling cluster switch log collection.
```

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

```
system switch ethernet log show
```



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

Resolución de problemas

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

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

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

Configurar SNMPv3

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

Acerca de esta tarea

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

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application  
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

El siguiente comando establece el nombre de usuario SNMPv3 con CSHM:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Pasos

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

```
show snmp user
```

Muestra el ejemplo

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

(sw1) (Config) # show snmp user

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

User                Auth                Priv(enforce)    Groups
acl_filter
-----
-----
admin               md5                des(no)          network-admin
SNMPv3User          md5                aes-128(no)      network-operator
-----
-----

      NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

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

(sw1) (Config) #
```

2. Configure el usuario SNMPv3 en el lado ONTAP:

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


Muestra el ejemplo

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

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

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

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

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

Enter the authentication protocol password again:

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

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

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

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

Muestra el ejemplo

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

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N9K-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
```

Muestra el ejemplo

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

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

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-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::*>
```

Sustituya un switch de almacenamiento Cisco Nexus 9336C-FX2

Es posible sustituir un switch Nexus 9336C-FX2 defectuoso en una red de clúster. Se trata de un procedimiento no disruptivo.

Lo que necesitará

Antes de instalar el software NX-OS y los RCF en un switch de almacenamiento Cisco Nexus 9336C-FX2, asegúrese de que:

- Su sistema es compatible con los switches de almacenamiento Cisco Nexus 9336C-FX2.
- 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
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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