Actualización del software NX-OS de Nexus 5500 y 5600

Contenido

- Introducción
- Prerequisites
  - Hardware aplicable
  - Software NX-OS
  - Códigos mínimos recomendados
- Antecedentes
  - In-Service Software Upgrade (ISSU)
    - Consideraciones
    - Prerrequisitos de ISSU
    - Servicios de gestión durante ISSU
  - Actualización de software no en servicio (no ISSU)
    - Motivos de la actualización disruptiva
- Rutas de actualización admitidas
- Métodos admitidos para actualizar
  - ISSU (sin interrupciones)
  - Sin ISSU (disruptivo)
- Documentación relacionada

Introducción

Este documento describe las opciones de actualización y las rutas para el software NX-OS de un switch Nexus de Cisco serie 5500 y 5600.

Prerequisites

Hardware aplicable

La información cubierta en este documento se aplica a este hardware solamente:

- Cisco Nexus 5596UP
- Cisco Nexus 5596T
- Cisco Nexus 5548UP
- Cisco Nexus 5548P
- Cisco Nexus 5672UP
- Cisco Nexus 5648Q
- Cisco Nexus 5624Q
- Cisco Nexus 5696Q

- Cisco Nexus 56128

Software NX-OS

El software NX-OS para los switches Nexus de las series 5500 y 5600 consta de kickstart and system images . Al actualizar el software NX-OS del dispositivo, asegúrese de que ambas imágenes coinciden con la misma versión.

Para obtener las imágenes de NX-OS necesarias:

- Vaya al Centro de descarga de software en https://software.cisco.com/download/home .
- Busque la plataforma Nexus 5500 y 5600 correspondiente que debe actualizarse.
- Descargue tanto la imagen del sistema como la de kickstart para el código que debe instalarse en el dispositivo.

Códigos mínimos recomendados

Para obtener información mínima sobre las versiones recomendadas del software NX-OS para los switches Nexus de Cisco serie 5500 y 5600, consulte uno de estos documentos aplicables:

Versiones mínimas recomendadas de Cisco NX-OS para switches Nexus de Cisco serie 5500

Versiones mínimas recomendadas de Cisco NX-OS para switches Nexus de Cisco serie 5600

Antecedentes

Los switches Nexus de Cisco series 5500 y 5600 ofrecen dos opciones diferentes para actualizar el software: In Service Software Upgrade (ISSU) y Non-ISSU. Cada opción se puede aprovechar en función del entorno, la configuración aplicada y el tiempo de inactividad que se permita.

In-Service Software Upgrade (ISSU)

Los switches Nexus de Cisco serie 5500 y 5600 admiten una única arquitectura ISSU de "supervisor" y realizan un reinicio stateful de todo el sistema operativo tras la ejecución, al tiempo que dejan intacto el reenvío del plano de datos. Durante este tiempo, las funciones del plano de control del switch sometido a ISSU se suspenden temporalmente durante 80 segundos y los cambios de configuración no se permiten.

Consideraciones

- ISSU sólo se admite entre imágenes compatibles. Vea la sección Rutas de Actualización Soportadas de este documento.
- Cualquier falla desde el punto en que ISSU no se puede abortar correctamente puede resultar en una actualización disruptiva (recarga del chasis). Las razones comunes para la interrupción de ISSU son inserciones y remociones de módulos o cambios en la topología del árbol de expansión mientras el switch está en proceso de ISSU.

- Un ISSU exitoso no causa ninguna recarga en el chasis ni en ningún FEX conectado.

- Las solicitudes de cambio de configuración de CLI y SNMP son denegadas durante las operaciones de ISSU.

Prerrequisitos de ISSU

A continuación se muestra una lista de requisitos que deben cumplirse para que ISSU sea compatible; si no cumple uno de ellos, es suficiente con que ISSU falle:

- El dispositivo no debe ejecutar servicios de capa 3. Debe desconfigurar todas las funciones de Capa 3, eliminar la licencia L3 y recargar el switch para tener una actualización no disruptiva con un ISSU.

- Los temporizadores LACP rápidos (hello=1 sec, dead=3 sec) no son compatibles con ISSU. Los temporizadores predeterminados (hello=30 sec, dead=90 sec) se deben configurar en el switch y sus vecinos LACP.

- Los switches habilitados para STP no pueden estar presentes en el flujo descendente del switch que se encuentra en una ISSU.

- La función STP Bridge Assurance (**spanning-tree port type network**) no se puede configurar en ninguna interfaz excepto en el enlace de par vPC.

- Ningún cambio de topología debe estar activo en ninguna instancia de STP.

- No puede haber ninguna interfaz en el estado de reenvío designado STP excepto el enlace par VPC. Si hay alguna interfaz en este estado y está conectada a dispositivos que no ejecutan STP, como servidores, routers, firewalls y otros, puede configurar spanning-tree port type edge en los puertos de acceso y en los puertos troncales para cumplir con el requisito. No utilice spanning-tree port type edge en interfaces que se conectan a switches que ejecutan STP.

- En el caso de una configuración VPC, todos los requisitos previos de ISSU deben cumplirse en ambos pares VPC simultáneamente.

Servicios de gestión durante ISSU

Antes de reiniciar el switch para ISSU (el plano de control se desactiva durante ~80 segundos), inband and management connections are brought down, and are brought back up after ISSU completes. Los servicios que dependen de los puertos de administración y dentro de la banda se ven afectados durante este tiempo, por ejemplo: las sesiones Telnet, SSH, AAA, RADIUS, HTTP y NTP hacia y desde el switch se interrumpen durante el reinicio del plano de control ISSU. Por esta razón, se recomienda tener acceso a la consola durante el proceso ISSU, de modo que el usuario pueda seguir observando el progreso de ISSU mientras las conexiones de administración regresan.

Actualización de software no en servicio (no ISSU)

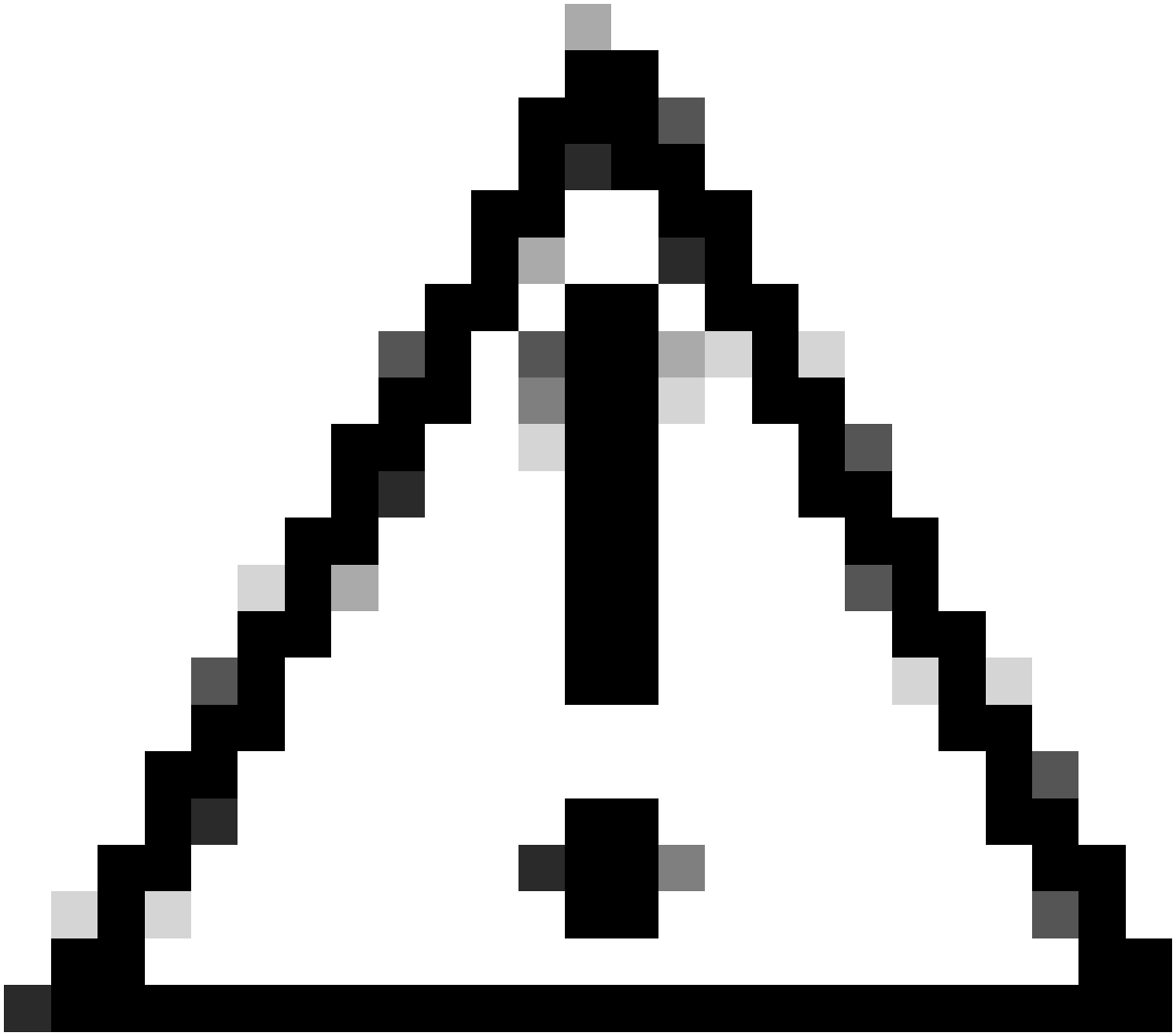
Los switches Nexus de Cisco serie 5500 y 5600 también admiten una opción que no es ISSU, conocida comúnmente como actualización disruptiva, que permite cargar una nueva imagen recargando el dispositivo.

Motivos de la actualización disruptiva

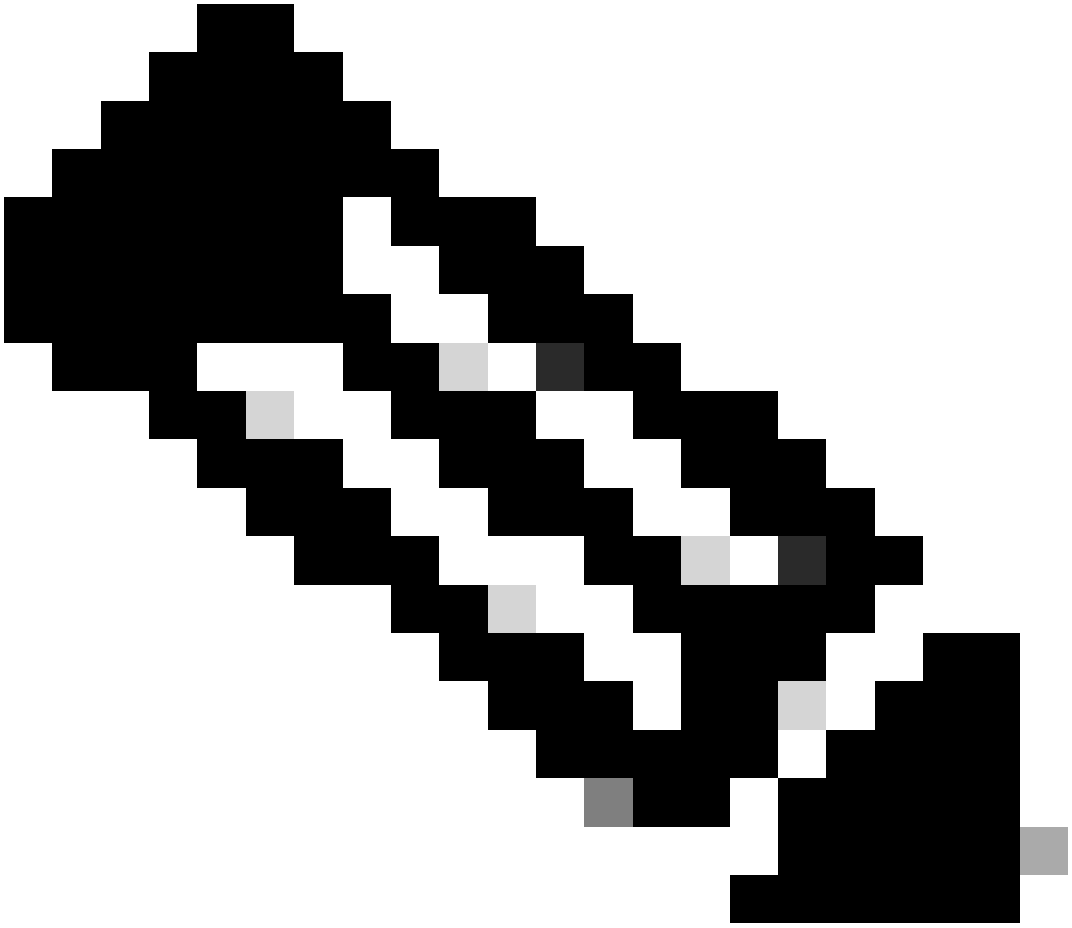
- La actualización disruptiva es el único método para actualizar si no se cumple una de las condiciones de ISSU.

- Con una actualización disruptiva, todos los FEX conectados se actualizan simultáneamente, por lo que el período de mantenimiento puede ser más corto.

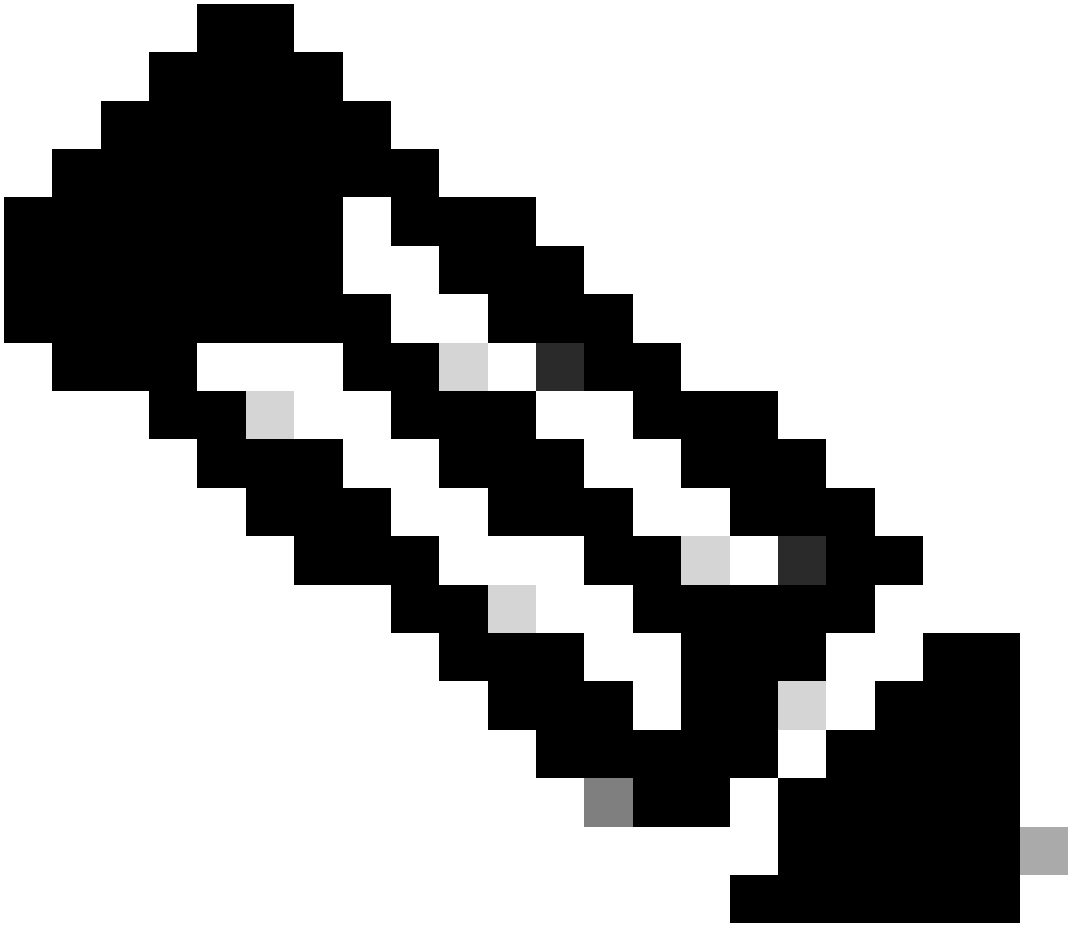
- Se pueden realizar actualizaciones disruptivas entre imágenes incompatibles, lo que puede ayudar a evitar varios saltos de actualización que requiere la opción ISSU.



Precaución: la ejecución de una actualización entre imágenes incompatibles puede ocasionar cierta pérdida de la configuración. Consulte ID de bug de Cisco CSCul2703 para obtener detalles. Se debe decidir si es aceptable perder parte de la configuración y restaurarla después de la actualización o si se prefiere conservar toda la configuración mediante una ruta de actualización admitida.



Nota: Si actualiza desde cualquier versión 7. x a una versión que tiene una corrección del Id. de bug Cisco CSCva49522**, se utiliza la reproducción de configuración binaria y no se espera una pérdida de configuración.**



Nota: los switches Nexus 5596 no se pueden iniciar tras una recarga o una actualización de NX-OS si no se ha actualizado la configuración del controlador de alimentación. Consulte Cisco bug ID CSCun6310 para obtener más detalles.

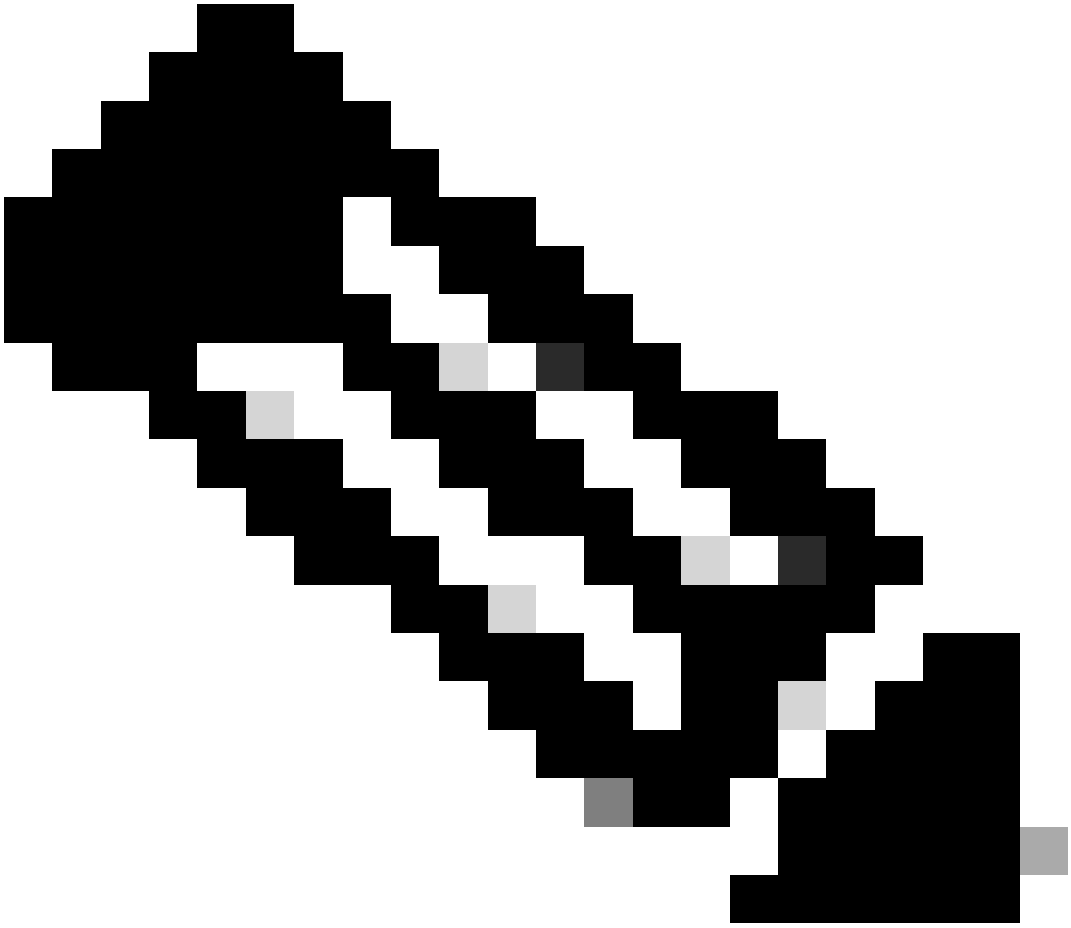
Rutas de actualización admitidas

Consulte la tabla 1 para conocer las rutas de actualización compatibles con Cisco NX-OS versión 7.3(13)N1(1) y 7.3(14)N1(1) en Nexus 5500.

Tabla 1. Rutas de actualización admitidas para Cisco Nexus 5500

Versión actual	Versiones intermedias	Versión de

		destino
Cualquier versión de Cisco NX-OS 7.3	Compatibilidad con actualización directa	7.3(13)N1(1) 7.3(14)N1(1)
Cualquier versión de Cisco NX-OS 7.2	7.3(2)N1(1)	
NX-OX 7.1(4) o 7.1(5)	Compatibilidad con actualización directa	
NX-OX 7.1 antes de 7.1(4)	7.1(4)N1(1) o 7.1(5)N1(1)	
NX-OX 7.0(4) o superior	7.1(4)N1(1) o 7.1(5)N1(1)	
NX-OX 7.0 antes de 7.0(4)	Dos saltos: primero 7.0(8)N1(1) y después 7.1(4)N1(1)	
NX-OX 5.2 o 6.0	Dos saltos: primero 7.0(4)N1(1) y luego a 7.1(4)N1(1)	



Nota: No puede actualizar sin interrupciones a Cisco NX-OS Release 7.3(13)N1(1) desde Cisco NX-OS Release 7.3(7)N1(1) debido al problema debido al Id. de error de Cisco CSCvt58479.

Consulte la tabla 2 para ver las rutas de actualización compatibles con Cisco NX-OS versión 7.3(13)N1(1) y 7.3(14)N1(1) en Nexus 5600.

Tabla 2. Rutas de actualización compatibles para los switches Nexus de Cisco serie 5600

Versión actual	Versiones intermedias	Versión de destino

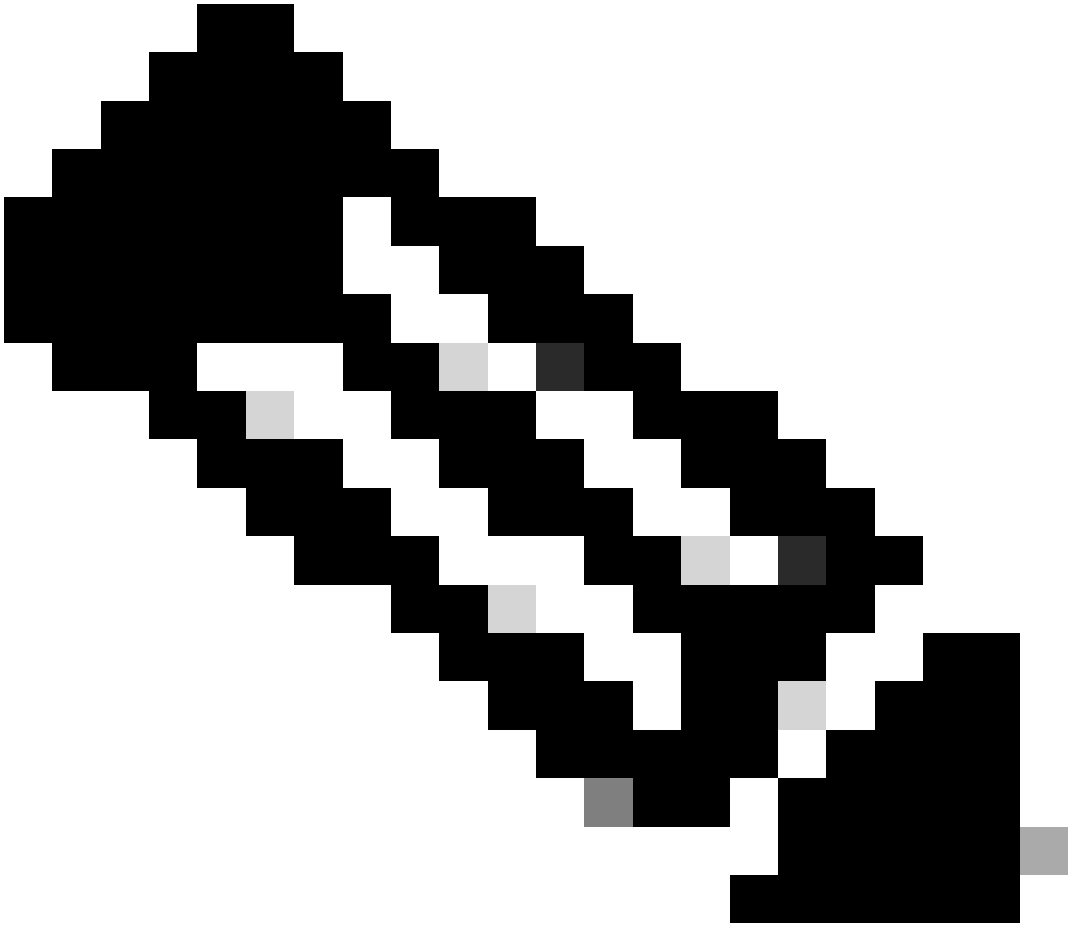
Cualquier versión superior a 7.3(8)N1(1)	Compatibilidad con actualización directa	7.3(13)N1(1) 7.3(14)N1(1)
NX-OS 7.2(1)N1(1)	Dos saltos: primero 7.3(2)N1(1), luego 7.3(8)N1(1)	
NX-OS 7.2(0)N1(1)	Tres saltos: primero 7.2(1)N1(1), después 7.3(2)N1(1), después 7.3(8)N1(1)	
NX-OX 7.1(4) o 7.1(5)	7.3(8)N1(1)	
NX-OX 7.1 antes de 7.1(4)	7.1(4)N1(1) o 7.1(5)N1(1)	
NX-OX 7.0(4) o superior	7.1(4)N1(1) o 7.1(5)N1(1)	
NX-OX 7.0 antes de 7.0(4)	Dos saltos: primero 7.0(8)N1(1) y después 7.1(4)N1(1)	

Métodos admitidos para actualizar

ISSU (sin interrupciones)

Para activar una actualización ISSU, se debe utilizar elinstall all comando entre imágenes compatibles:

switch# install all kickstart bootflash:[kickstart-image.bin] system bootflash:[system-image.bin]



Nota: para obtener información adicional sobre los pasos de actualización de los switches Nexus de Cisco serie 5500 y 5600, seleccione la guía de actualización correspondiente de la Guía de actualización y reducción del software Cisco Nexus serie 5X00 NX-OS y consulte la sección **Procedimientos de actualización**.

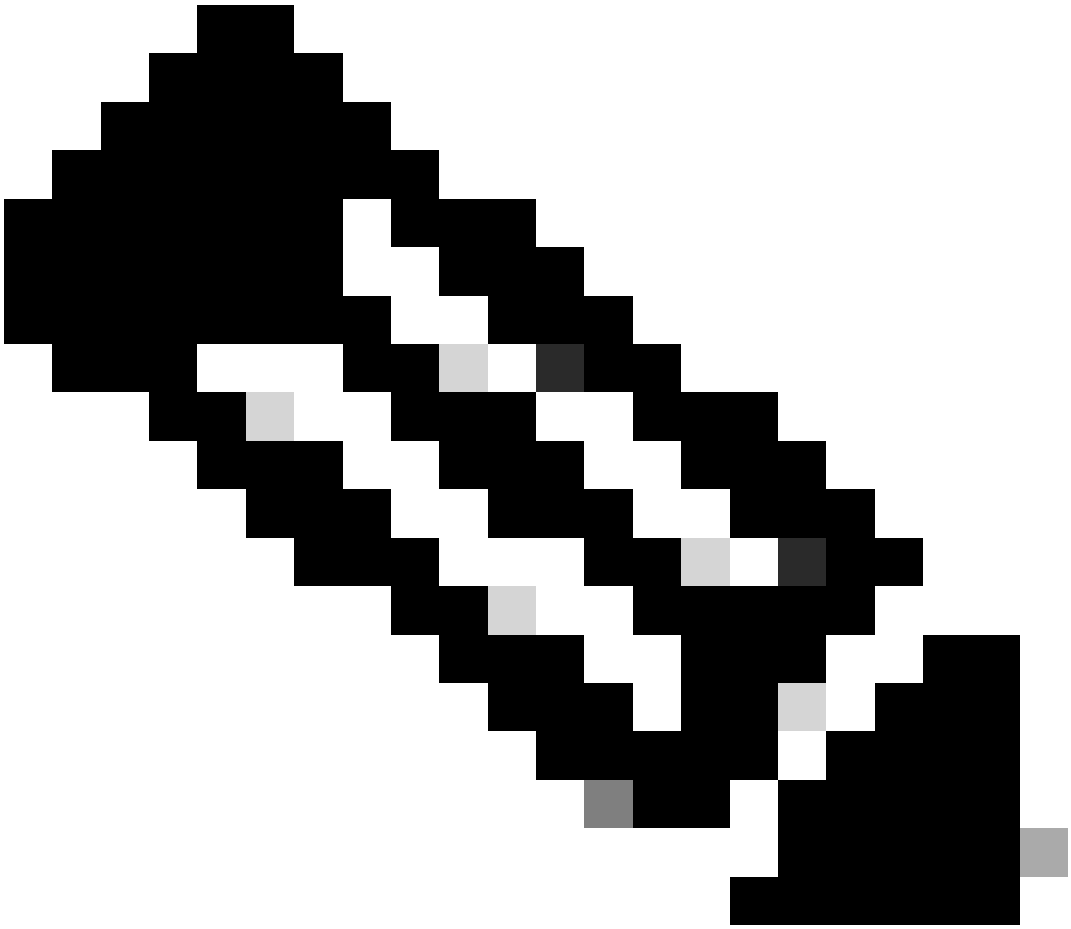
Sin ISSU (disruptivo)

Para activar una actualización que no sea ISSU, se debe utilizar elinstall all comando entre imágenes compatibles o incompatibles:

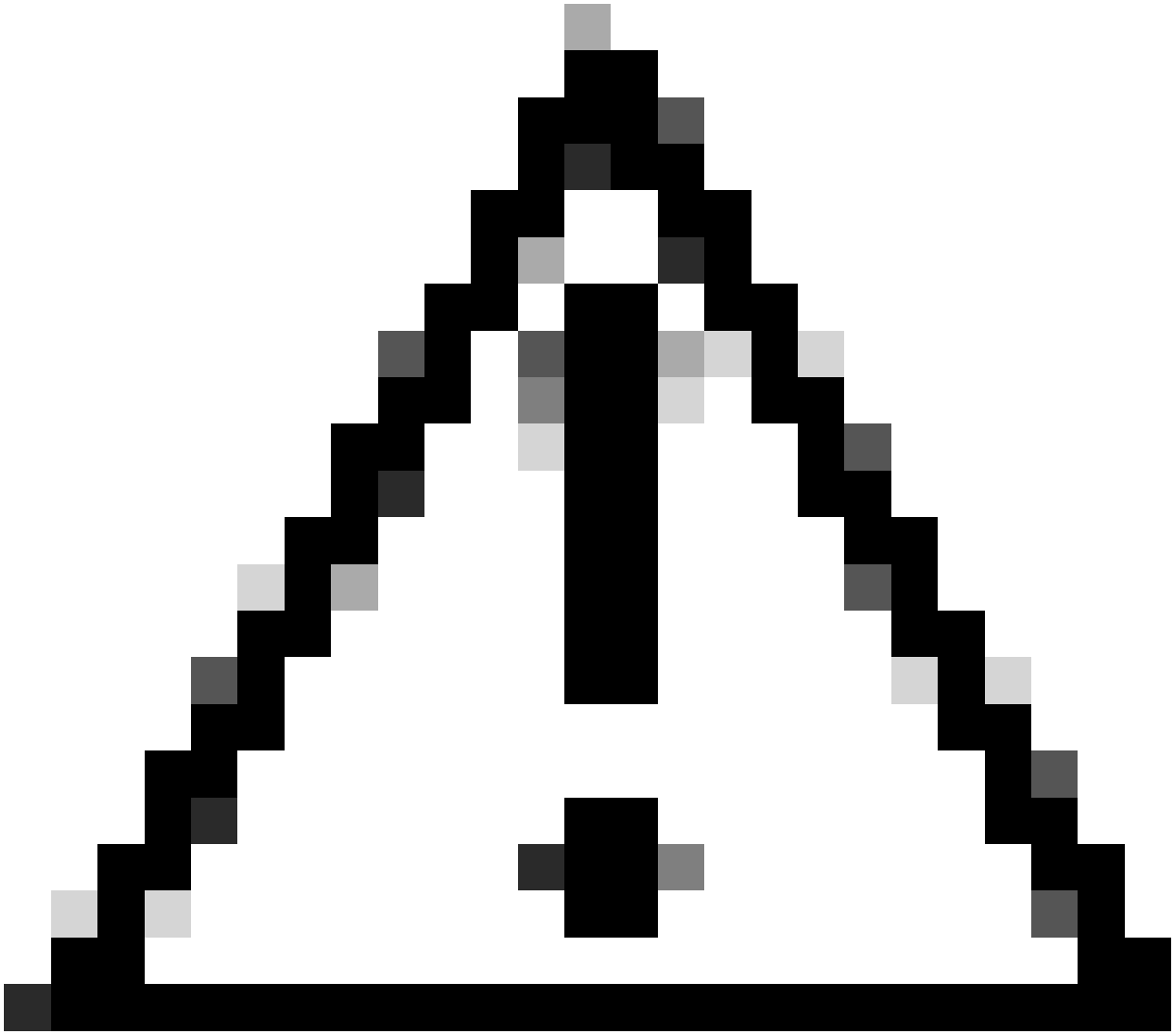
switch# install all kickstart bootflash:[kickstart-image.bin] system bootflash:[system-image.bin]

Para forzar una actualización disruptiva incluso si se puede aprovechar un ISSU, utilice install all el comando con la force opción:

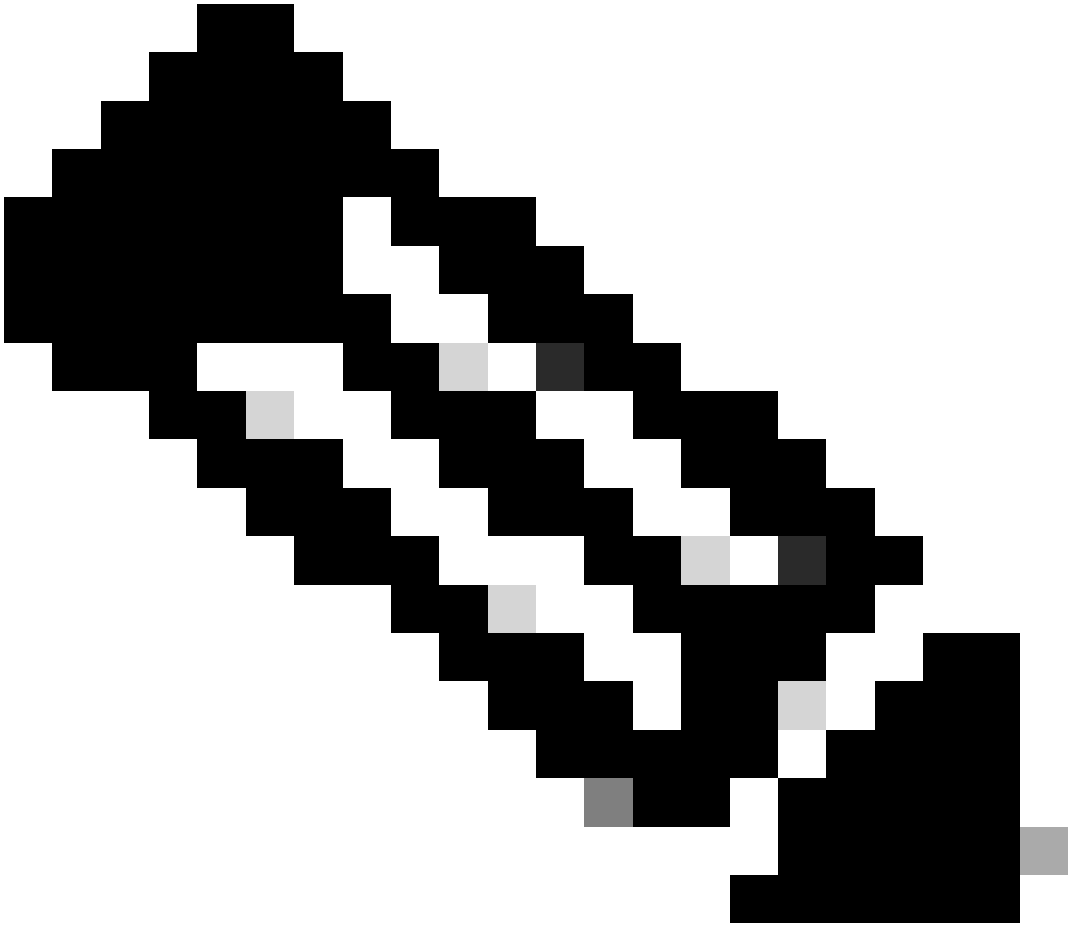
switch# install all force kickstart bootflash:[kickstart-image.bin] system bootflash:[system-image.bin]



Nota: Después de que el comando install all complete sus comprobaciones previas, se alerta a una actualización disruptiva con este mensaje: Switch will be reloaded for disruptive upgrade. Do you want to continue with the installation (y/n)? [n]escriba 'y' para que la actualización continúe.



Precaución: no se recomienda cambiar la variable de arranque para actualizar o actualizar a una versión anterior de Cisco NX-OS. Esto puede provocar la pérdida de la configuración y la inestabilidad del sistema.



Nota: para obtener información adicional sobre los pasos de actualización de los switches Nexus de Cisco serie 5500 y 5600, seleccione la guía de actualización correspondiente de la Guía de actualización y reversión del software Cisco Nexus serie 5X00 NX-OS y consulte la sección **Procedimientos de actualización.**

Documentación relacionada

La documentación de los switches Nexus de Cisco serie 5500 y 5600 está disponible en los switches Nexus de Cisco serie 5000.

El conjunto de documentación se divide en las siguientes categorías:

    - Release Notes
- Guías de instalación y actualización
- Referencias de Comando
- Guías de Configuración
- Mensajes de error y del sistema

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).