Realización de un restablecimiento de fábrica seguro en routers periféricos SD-WAN

Contenido

Introducción

Este documento describe el procedimiento de restablecimiento de fábrica seguro para Cisco Catalyst SD-WAN Edge Routers que ejecutan Cisco IOS® XE.

Background

Un restablecimiento de fábrica devuelve el dispositivo a su estado de fabricación original y suele ser necesario como parte de los flujos de trabajo de retirada del servicio, reimplementación o remediación de seguridad.

⚠ Precaución: En este artículo se recomienda exclusivamente la opción `factory-reset all secure`, que realiza el saneamiento de datos alineados con NIST SP 800-88 Rev. 1. Este método hace que los datos de los medios de almacenamiento sean irrecuperables y proporciona el nivel más alto de garantía de que los datos confidenciales se han eliminado de forma permanente.

Aplicabilidad

El comando `factory-reset all secure` se soporta en estas plataformas que ejecutan Cisco IOS XE:

- Plataformas periféricas Cisco Catalyst serie 8200
- Plataformas periféricas Cisco Catalyst serie 8300
- Plataformas periféricas Cisco Catalyst serie 8500
- Routers de Servicios de Agregación Cisco ASR 1000 Series
- Routers de servicios integrados Cisco ISR serie 4000
- Routers de servicios integrados Cisco ISR serie 1000

 Nota: La opción `all secure` solo puede utilizarse en dispositivos independientes. Verifique que su plataforma y la versión de Cisco IOS XE admita la palabra clave `secure` al marcar `factory-reset ?` en modo EXEC privilegiado antes de continuar.

Prerequisites

Antes de realizar el restablecimiento de fábrica seguro, asegúrese de que se cumplen estos requisitos previos:

- Configuración de respaldo: Exporte y almacene de forma segura todas las configuraciones de dispositivos, plantillas y políticas desde el Administrador de SD-WAN (vManage) antes del restablecimiento.
- Imágenes de software de backup: Asegúrese de tener una copia de la imagen del software Cisco IOS XE cargada en la memoria de inicialización antes de realizar el restablecimiento. Mientras que la opción `secure` conserva la imagen de inicio en flash en la mayoría de las plataformas, ciertas plataformas limpian la memoria flash de inicio completamente como parte del borrado seguro. Como contingencia, tenga siempre la imagen de Cisco IOS XE disponible en una unidad USB o en un servidor TFTP accesible para garantizar la recuperación independientemente del comportamiento de la plataforma.
- Alimentación ininterrumpida: Asegúrese de que el dispositivo tenga una fuente de

alimentación ininterrumpida durante todo el proceso de reinicio. La pérdida de energía durante la desinfección puede hacer que el dispositivo sea irrecuperable.
- Complete cualquier procedimiento ISSU: Si hay alguna operación de actualización de software en funcionamiento (ISSU) pendiente o en curso, debe completarla antes de iniciar el restablecimiento de fábrica.
- Liberar licencia HSEC: La licencia HSEC debe liberarse del dispositivo antes de realizar el restablecimiento de fábrica. Devuelva la licencia de HSECK9 como se describe en la sección "Devolución de la licencia de HSECK9" en: Configuración de la licencia de HSECK9 en los routers periféricos de Cisco
- Eliminar del fabric SD-WAN: Invalide el certificado del dispositivo de vManage y quite el dispositivo de la superposición del controlador antes de realizar el restablecimiento.
- Acceso a consola: Asegúrese de tener acceso físico a la consola del dispositivo. Después del reinicio, el dispositivo entra en modo ROMMON y las sesiones VTY no están disponibles.

Consejo: Confirme que la imagen de Cisco IOS XE esté cargada en bootflash y que haya una copia de recuperación disponible en USB o TFTP antes de ejecutar el restablecimiento de fábrica. Mientras que la opción `secure` retiene la imagen de inicio en la mayoría de las plataformas, algunas plataformas sanean la memoria de inicialización completamente durante el proceso.

Lo que se borra

El comando `factory-reset all secure` elimina permanentemente estos datos del dispositivo:

Categoría	Datos borrados
Software	Todas las imágenes del software Cisco IOS XE (la imagen de inicio actual se conserva en flash en la mayoría de las plataformas; sin embargo, en ciertas plataformas, la memoria flash de inicialización se limpia por completo)
Configuración	Configuración de inicio, configuración en ejecución
Registros y diagnósticos	Información de fallos, registros del sistema, OBFL (registro de fallos integrado)
Material de seguridad	Claves y credenciales relacionadas con FIPS, claves PKI configuradas por el usuario y certificados
Almacenamiento	Todos los datos de usuario en almacenamiento extraíble (SATA, SSD, USB)
Licencias	Todas las licencias de dispositivos (se debe volver a registrar)
ROMMON	Variables de entorno ROMMON agregadas por el usuario

Nota: Estos elementos se conservan después del restablecimiento seguro de fábrica:

- Certificados SUDI (Identificador de dispositivo único seguro) y claves PKI asociadas
- Valor del registro de configuración
- La imagen de arranque actual (conservada en flash en la mayoría de las plataformas; en ciertas plataformas, la memoria de inicialización está completamente desinfectada (siempre se realiza la recuperación de USB/TFTP)

Procedimiento: Reinicio seguro de fábrica

Advertencia: Este procedimiento es irreversible. Una vez iniciado, todos los datos enumerados en la tabla anterior se destruyen permanentemente. Asegúrese de que se han verificado todas las copias de seguridad antes de continuar.

Paso 1: Acceso al dispositivo a través de la consola

Conéctese al dispositivo mediante una conexión de consola física. El acceso SSH/VTY se pierde durante el proceso de restablecimiento.

Paso 2: Introducir modo EXEC privilegiado

```
Device> enable
Device#
```

Paso 3: Ejecución del restablecimiento seguro de fábrica

Ejecute este comando para iniciar el restablecimiento de fábrica seguro:

```
Device# factory-reset all secure
```

El sistema solicita confirmación:

```
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
```

⚠ Comprobar: En el mensaje de confirmación, compruebe por última vez que:

- Se ha realizado una copia de seguridad de todas las configuraciones
- La imagen de recuperación de Cisco IOS XE está disponible en USB o TFTP
- El dispositivo se ha eliminado de la superposición SD-WAN

Escriba `y` o presione Enter para confirmar y continuar.

Paso 4: Espere a que finalice la desinfección

El dispositivo realiza la desinfección de los datos en todos los medios de almacenamiento. Este proceso puede durar un periodo prolongado en función de la capacidad de almacenamiento. No interrumpa la alimentación durante esta operación.

Al finalizar, el dispositivo se recarga automáticamente e ingresa en el modo ROMMON.

Paso 5: Restaurar variables de entorno ROMMON

Después del restablecimiento, las variables de entorno, incluidas `MAC_ADDRESS` y `SERIAL_NUMBER`, se pueden borrar. Realice un restablecimiento de ROMMON para restaurarlos:

```
rommon 1> reset
```

✎ Nota: La variable de entorno de velocidad en BAUD vuelve a su valor predeterminado (9600) después de un restablecimiento de fábrica. Si la sesión de consola se configuró a una velocidad en baudios diferente, puede ajustar la configuración del emulador de terminal a 9600 baudios para recuperar el acceso a la consola.

Paso 6: Iniciar la imagen del software Cisco IOS XE

En la mayoría de las plataformas, la opción `secure` conserva la imagen de inicio en flash. Verifique su presencia con `dir bootflash:` de ROMMON. Si la imagen está disponible, inicie directamente:

```
rommon 2> boot bootflash:<image-filename>.bin
```

Comportamiento específico de la plataforma: En ciertas plataformas de hardware, el proceso de saneamiento seguro borra totalmente la memoria de inicialización, incluida la imagen de inicio. En estos casos, recupere a través de USB o TFTP.

Opción A — Recuperación mediante USB:

```
rommon 2> boot usbflash0:<image-filename>.bin
```

Opción B — Recuperación TFTP:

Establezca las variables de entorno ROMMON necesarias y, a continuación, inicie la transferencia:

```
rommon 2> IP_ADDRESS=

rommon 3> IP_SUBNET_MASK=

rommon 4> DEFAULT_GATEWAY=

rommon 5> TFTP_SERVER=

rommon 6> TFTP_FILE=

     .bin
rommon 7> tftpboot
```

Verifique que la conectividad con el servidor TFTP esté disponible a través de la interfaz de administración o de un segmento de red conectado directamente. ROMMON no admite protocolos de ruteo, por lo que el servidor TFTP debe ser accesible a través del gateway predeterminado configurado.

Tenga siempre una imagen de recuperación guardada en el puerto USB o un servidor TFTP accesible antes de iniciar el restablecimiento de fábrica para tener en cuenta este comportamiento.

Post-reinicio: Reincorporación a fabric de SD-WAN

Una vez que el dispositivo se haya restaurado con una imagen limpia de Cisco IOS XE, utilice los procedimientos de incorporación SD-WAN estándar para volver a introducir el dispositivo en el

fabric:

1. Configuración de Bootstrap: Aplique la configuración de arranque inicial (IP del sistema, ID del sitio, nombre de la organización, dirección de vBond). Consulte Generar archivo de Bootstrap mediante CLI para obtener información sobre el procedimiento.
2. Instalación del certificado: Instale el certificado del dispositivo y la cadena de CA raíz según lo requiera su autoridad de certificación (Symantec/DigiCert, Cisco PKI o Enterprise CA).
3. Conexiones de control: Verifique que las conexiones de control DTLS/TLS estén establecidas en vManage, vSmart y vBond.
4. Inserción de plantilla: En vManage, adjunte la plantilla de dispositivo o el grupo de configuración adecuados al dispositivo.
5. Validación: Confirme que las sesiones BFD, las rutas OMP y los túneles del plano de datos estén operativos.

Nota: Después de la reincorporación, la licencia HSEC (alta seguridad) se debe volver a aplicar manualmente a través de CLI para restaurar el rendimiento de cifrado. Como se documenta en Administración de licencias HSEC en Cisco Catalyst SD-WAN, SD-WAN Manager (vManage) no admite la reinstalación de una licencia HSEC en un dispositivo. Se requiere una recarga del dispositivo en los routers físicos para activar la licencia. Refiérase a Configuración de la Licencia HSECK9 en los Routers de Borde de Cisco para el procedimiento manual de CLI.

Resolución de problemas

La consola no responde después del reinicio

Si la consola no responde después de que se complete el restablecimiento de fábrica, es probable que la velocidad en baudios haya vuelto al valor predeterminado (9600). Ajuste el emulador de terminal a 9600 baudios y vuelva a conectar.

El dispositivo no ingresa a ROMMON

Si el dispositivo no ingresa a ROMMON después de que se complete el restablecimiento, verifique que el registro de configuración esté configurado correctamente. En la mayoría de los casos, un ciclo de alimentación fuerza al dispositivo a entrar en ROMMON cuando no hay una imagen de arranque presente.

Faltan variables de entorno en ROMMON

Si faltan las variables `MAC_ADDRESS` o `SERIAL_NUMBER` después del restablecimiento, ejecute el comando `reset` en ROMMON para restaurar las variables de entorno predeterminadas de fábrica del almacenamiento de hardware.

Preguntas Frecuentes

A: ¿Por qué se recomienda la opción "seguro" en lugar de las opciones estándar de "todos" o "tres pasos"?

R: La opción `factory-reset all secure` realiza el saneamiento de datos más completo disponible, alineado con NIST SP 800-88 Rev. 1. Hace que los datos sean irrecuperables y conserva la imagen de arranque actual en flash, lo que simplifica la recuperación. En comparación, la opción `3-pass` realiza un patrón de sobrescritura de tres pasadas (ceros, unos, aleatorio) que toma aproximadamente tres veces más de tiempo y también borra la imagen de inicio, lo que requiere una recarga completa de la imagen desde USB o TFTP. Se recomienda la opción `secure`, ya que proporciona el saneamiento más completo con el menor gasto operativo para la recuperación.

A: ¿Cuánto tarda el restablecimiento de fábrica seguro?

R: La duración varía en función de la capacidad de almacenamiento total del dispositivo. En el caso de dispositivos con almacenamiento flash estándar (8-32 GB), el proceso suele completarse en un plazo de 15-45 minutos. Los dispositivos con almacenamiento SSD o SATA de mayor tamaño pueden tardar más. Importante: No interrumpa la alimentación durante este proceso. Planifique una ventana de mantenimiento que tenga en cuenta el reinicio más la recarga de la imagen y el tiempo de reincorporación.

A: ¿El dispositivo conserva su identidad (número de serie, SUDI) después del reinicio?

R: Yes. El certificado de identificador único de dispositivo seguro (SUDI) y sus claves PKI asociadas se almacenan en un almacenamiento protegido por hardware (chip TAm/ACT2) y no se borran al restablecer los parámetros de fábrica. El número de serie del dispositivo también se conserva en el hardware. Esto significa que el dispositivo se puede volver a incorporar al fabric SD-WAN utilizando su identidad original después del reinicio.

A: ¿Es necesario quitar el dispositivo del Administrador de SD-WAN antes de realizar el restablecimiento?

R: Yes. Se recomienda enfáticamente invalidar el certificado del dispositivo y remover el dispositivo de la superposición SD-WAN antes de realizar el restablecimiento de fábrica. Esto garantiza una eliminación limpia de la infraestructura del controlador, sin entradas obsoletas en el inventario de dispositivos de vManage y sin conexiones de control huérfanas ni estado de túnel.

Desde vManage: Navegue hasta Configuration > Certificates > select the device > Invalidate, luego Send to Controllers. A continuación, elimine el dispositivo de la lista de dispositivos.

A: ¿Qué sucede con la licencia HSEC después del restablecimiento de fábrica?

R: La licencia HSEC (alta seguridad) se elimina durante el restablecimiento de fábrica. Sin ella, el dispositivo funciona con un rendimiento de cifrado restringido. La licencia HSEC debe ser liberada antes del restablecimiento de fábrica para que pueda ser reutilizada después:

1. Antes del reinicio: Libere la licencia a través de la `autorización inteligente de la licencia, devuelva la licencia local en línea` y elimine la instancia del producto de Smart License Central.
2. Después de la reincorporación: Vuelva a aplicar manualmente la licencia de HSEC mediante CLI. Como se documenta en Administración de licencias HSEC en Cisco Catalyst SD-WAN, SD-WAN Manager (vManage) no admite la reinstalación de la licencia HSEC.
3. Recargar: Se requiere una recarga en los routers físicos para activar la licencia.
4. Verifique a través de `show license summary` y `show license authorization`.

Para ver el procedimiento completo, consulte Configuración de la licencia HSECK9 en los routers periféricos de Cisco y Administración de licencias HSEC en Cisco Catalyst SD-WAN.

A: ¿Puedo realizar el restablecimiento de fábrica seguro de forma remota (mediante SSH/VTY)?

R: Aunque el comando se puede ejecutar técnicamente sobre una sesión SSH/VTY, se desaconseja fuertemente. El dispositivo comienza inmediatamente la desinfección y la sesión remota finaliza. Después del reinicio, el dispositivo ingresa en el modo ROMMON donde no hay conectividad IP disponible, no es posible el acceso VTY y se requiere acceso a la consola para la recuperación de la imagen. Asegúrese siempre de que el acceso a la consola física esté disponible antes de iniciar el restablecimiento de fábrica.

A: ¿Es el restablecimiento de fábrica seguro adecuado para los escenarios de remediación de seguridad?

R: Yes. El restablecimiento seguro de fábrica es el enfoque recomendado cuando se debe devolver un dispositivo a un estado de funcionalidad comprobada después de un riesgo sospechoso. Esto garantiza que se eliminen permanentemente todas las claves, puertas traseras o mecanismos de persistencia instalados por el atacante, que no queden datos residuales de configuración o credenciales y que se garantice que el dispositivo está limpio para la reincorporación. Para los reinicios de fábrica relacionados con la seguridad, asegúrese de que se generan nuevas credenciales (contraseñas, claves, certificados) durante la reincorporación y de que no se restauran en el dispositivo configuraciones de copia de seguridad que no estén en riesgo.

A: ¿Por qué no usar "request platform software sdwan software reset" o "request platform software sdwan config reset" en su lugar?

R: Estos comandos tienen un propósito diferente y no proporcionan el mismo nivel de saneamiento que `factory-reset all secure`. El comando `request platform software sdwan software reset` restablece la superposición del software SD-WAN pero no borra las configuraciones, claves, certificados o almacenamiento subyacentes de Cisco IOS XE, el dispositivo conserva su estado de SO base. El comando `request platform software sdwan config reset` restablece solamente la configuración SD-WAN pero deja intactos en el disco la imagen de Cisco IOS XE, las credenciales locales, las claves SSH y todos los demás datos. Ninguno de los comandos realiza la desinfección de datos en el medio de almacenamiento. Si el objetivo es devolver el dispositivo a un estado completamente limpio, especialmente después de un incidente de seguridad, estos comandos son insuficientes porque los datos residuales (claves, credenciales, registros, archivos plantados por atacantes) pueden permanecer en la memoria flash o SSD. Utilice `factory-reset all secure` cuando se debe garantizar que el dispositivo está limpio en el nivel de almacenamiento.

Referencias

- Cisco Trustworthy Systems: Guía de restablecimiento de fábrica
- Configuración de la licencia HSECK9 en los routers periféricos de Cisco
- Administración de licencias HSEC en Cisco Catalyst SD-WAN
- Generar archivo de Bootstrap mediante CLI: guía de inicio de SD-WAN
- Actualización de controladores SD-WAN con el uso de vManage GUI o CLI

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).