

Nuevo procedimiento de recuperación de contraseña en la plataforma Cisco 8000 y NCS5500

Contenido

[Introducción](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[Nuevos pasos de recuperación de contraseña](#)

[Summary](#)

Introducción

Este documento describe un nuevo proceso de recuperación de contraseña para Cisco IOS®-XR para las plataformas Cisco 8000 y NCS5500.

Antecedentes

Si un usuario olvida la contraseña raíz o las contraseñas de todos los usuarios se pierden en las plataformas XR7 LNT (Cisco 8000, NCS-540L) o eXR (ASR9K de 64 bits, NCS5K, NCS5500, NCS 540 y NCS 560), el router se vuelve inaccesible para el usuario ya que el inicio de sesión no es posible sin la combinación correcta de nombre de usuario y contraseña. Hoy en día, la recuperación de la contraseña de tal router sólo es posible a través de la recreación de la imagen del router con el uso del método de arranque USB o el arranque iPXE desde un servidor externo. La recreación de la imagen del router implica volver a instalar el software del router y cargar la configuración del dispositivo. La instalación del software es un proceso que lleva mucho tiempo.

A partir de la versión 7.3.16 para la plataforma de la serie Cisco 8000 y 7.3.3 para la plataforma de la serie NCS5500, Cisco ha presentado un nuevo método para la recuperación de contraseñas sin necesidad de volver a crear imágenes del router. Este método de recuperación de contraseña no requiere que se vuelva a instalar el software, lo que ahorra tiempo y permite el acceso al reinicio de la contraseña posterior del router. Este nuevo método de recuperación de contraseña cumple con los estándares de seguridad, ya que la información de usuario antigua y los datos de tiempo de ejecución de usuario se eliminan antes de iniciar el proceso de recuperación de contraseña.

Problema

Hoy en día, la recuperación de contraseñas en plataformas XR7 LNT (Cisco 8000, NCS-540L) o eXR (ASR9K de 64 bits, NCS5K, NCS5500, NCS 540 y NCS 560) no es posible. La única alternativa disponible para restablecer la contraseña es recrear la imagen del router con el uso del método de arranque USB o arranque iPXE desde un servidor externo. Se trata de un proceso que lleva mucho tiempo, ya que implica volver a instalar el software del router y cargar la

configuración del dispositivo.

Se necesita un método más rápido y seguro para la recuperación de contraseñas en las plataformas Cisco XR7 y eXR.

Solución

A partir de la versión 7.3.16 para la plataforma de la serie Cisco 8000 y 7.3.3 para la plataforma de la serie NCS5500, Cisco ha presentado un nuevo método para la recuperación de contraseñas sin necesidad de volver a crear imágenes del router. En el menú Grand Unified Bootloader (GRUB) de la pantalla de inicio del procesador de routing (RP), se agrega una nueva opción: "IOS-XR-Recovery", que se crea explícitamente para el procedimiento de recuperación de contraseña. En la configuración del router, se crea un nuevo comando **system recovery** para habilitar la nueva función de recuperación de contraseña. Esta función es actualmente opcional y no está activada de forma predeterminada.

Advertencias:

- La opción de menú de pantalla GRUB de arranque del BIOS RP **IOS-XR-recovery** se verá independientemente del comando **system recovery** configurado o no configurado en la configuración del router. Si el comando **system recovery** no está presente en la configuración del router y se intenta un nuevo método de recuperación de contraseña seleccionando la opción de menú de pantalla del BIOS GRUB **IOS-XR-recovery**, el router anulará el proceso de recuperación de contraseña y arrancará con la configuración anterior. Por lo tanto, es obligatorio tener un comando **system recovery** configurado en el router para que el método de recuperación de contraseña funcione.
- La función de recuperación de contraseña está desactivada de forma predeterminada.
- La función de recuperación de contraseña debe habilitarse explícitamente mediante la interfaz de línea de comandos (CLI) de configuración.
RP/0/RP0/CPU0:HOSTNAME(config)#**recuperación del sistema.**
- Si el router experimenta un procedimiento de recuperación de contraseña, el comando **system recovery** se inhabilitará después del inicio del router, ya que toda la configuración del router se eliminaría como parte del procedimiento de recuperación de contraseña. Los usuarios deben cargar la configuración del dispositivo de nuevo y configurar el comando **system recovery** si no forma parte de la configuración del dispositivo.
- Aparte de la eliminación de la configuración del router, todos los archivos creados por el usuario, show tech files, dumper files se eliminarán del disco 0 y del disco duro como parte del procedimiento de limpieza durante la recuperación de la contraseña.
- Esta función se soporta actualmente en la versión 7.3.16 y superiores en Cisco 8000, 7.3.3 y superiores en NCS5500, y para otras plataformas XR7 LNT y eXR, esta función estará disponible en futuras versiones.
- Utilice el procedimiento dado para las plataformas donde ambas tarjetas RP están instaladas en el chasis. Traiga ambas tarjetas RP al menú del BIOS GRUB. A continuación, los procedimientos de recuperación de contraseña deben realizarse en cada tarjeta RP uno por uno. Este es un paso obligatorio para las plataformas RP duales, de lo contrario, conduciría a inconsistencias en la configuración y la limpieza de archivos.

Nuevos pasos de recuperación de contraseña

Requisito previo: La nueva función de recuperación de contraseña funciona sólo si la CLI forma parte de la configuración del dispositivo. Si la CLI no está configurada, el nuevo mecanismo de recuperación de contraseña no funcionará debido a la configuración CLI faltante.

Habilitar la función de recuperación de contraseña:

```
RP/0/RP0/CPU0:HOSTNAME(config)#system recovery
```

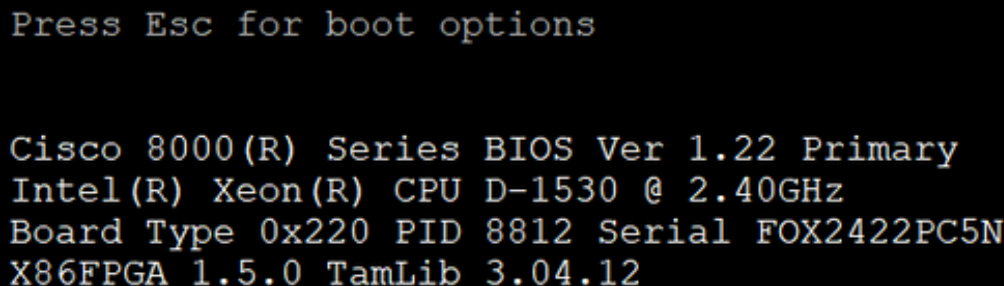
Desactivar la función de recuperación de contraseña:

```
RP/0/RP0/CPU0:HOSTNAME(config)#no system recovery
```

El procedimiento de recuperación de contraseña se debe realizar sólo a través de la consola RP.

Paso 1. Traiga la tarjeta RP al menú GRUB del bios. Para las plataformas en las que ambas tarjetas RP están instaladas en el chasis, ambas tarjetas RP se deben bajar al menú GRUB del bios antes de iniciar el procedimiento de recuperación de contraseña. Este es un paso obligatorio. Esto se puede hacer mediante un ciclo de energía del dispositivo y luego presione la tecla ESC en ambas consolas RP para ingresar el menú GRUB del bios o reubicando físicamente cada RP uno por uno y luego presione la tecla **ESC** en la consola RP para ingresar el menú GRUB del bios.

Tarjeta RP0 y RP1:

A screenshot of a BIOS boot options menu. The text is displayed in a monospaced font on a black background. At the top, it says "Press Esc for boot options". Below that, it lists system information: "Cisco 8000(R) Series BIOS Ver 1.22 Primary", "Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz", "Board Type 0x220 PID 8812 Serial FOX2422PC5N", and "X86FPGA 1.5.0 TamLib 3.04.12". A small green cursor is visible at the bottom left of the text area.

```
Press Esc for boot options

Cisco 8000(R) Series BIOS Ver 1.22 Primary
Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz
Board Type 0x220 PID 8812 Serial FOX2422PC5N
X86FPGA 1.5.0 TamLib 3.04.12
```

Tarjeta RP0 y RP1:

```
Press Esc for boot options
                        GNU GRUB  version 2.02 (LOCKED)

C+-----+
I| *IOS-XR-latest
B|  IOS-XR-fallback
X|  IOS-XR-recovery
|
W|
V|
(|
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS.
```

Paso 2. En la consola de la tarjeta RP0, seleccione la opción **IOS-XR-recovery** del menú GRUB y presione **Enter**.

Tarjeta RP0:

```
Press Esc for boot options
                        GNU GRUB  version 2.02 (LOCKED)

C+-----+
I|  IOS-XR-latest
B|  IOS-XR-fallback
X| *IOS-XR-recovery
|
W|
V|
(|
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS.
```

Paso 3. Seleccione la opción **IOS-XR-recovery** del menú GRUB y presione **Enter** en la consola de la tarjeta RP1, tan pronto como vea Iniciando la recuperación del sistema IOS-XR... mensaje en la consola de la tarjeta RP0. No espere hasta que la tarjeta RP0 llegue al mensaje "Enter root-system username:", de lo contrario la tarjeta RP1 se recargará automáticamente y saldrá del menú bios GRUB. La tarjeta RP0 se iniciará como activa y la tarjeta RP1 se iniciará como una tarjeta standby luego del proceso de recuperación.

Tarjeta RP0:

```

Execute: cryptsetup luksOpen /dev/main-xr-vg/install-data-encrypted_in encrypted -d '-'
#####
#           Initiating IOS-XR System Recovery...           #
# This will erase all user & system configuration! #
# *** System will reboot upon completion *** #
#####

Checking if system recovery is enabled
WARNING: Failed to connect to lvmtool. Falling back to device scanning.
System Recovery enabled by user
Start System Recovery

```

Tarjeta RP1:

```

Press Esc for boot options
                        GNU GRUB  version 2.02 (LOCKED)

C+-----+
I| IOS-XR-latest
B| IOS-XR-fallback
X| *IOS-XR-recovery
|
|
V|
( |
|
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS.

```

Paso 4. En la tarjeta RP0, cree un nuevo usuario y contraseña raíz. Intente iniciar sesión en el dispositivo con el uso del nuevo nombre de usuario y contraseña raíz.

Tarjeta RP0:

```

RP/0/RP0/CPU0:Jul  8 04:52:06.168 CEST: ifmgr[361]: %PKT_INFRA-LINK-3-UPDOWN : Interface MgmtEth0/RP0/CPU0/0, changed state to Down
RP/0/RP0/CPU0:Jul  8 04:52:06.170 CEST: ifmgr[361]: %PKT_INFRA-LINK-3-UPDOWN : Interface MgmtEth0/RP0/CPU0/0, changed state to Up

!!!!!!!!!!!!!!!!!!!!!! NO root-system username is configured. Need to configure root-system username. !!!!!!!!!!!!!!!!!!!!!!!

--- Administrative User Dialog ---

Enter root-system username: █

```

Paso 5. El procedimiento de recuperación de contraseña está completo en este momento.

El router se inicia ahora con una configuración en blanco y con el nombre de usuario/contraseña raíz creado en el paso 4. Continúe con la configuración normal del router o cargue una configuración desde un archivo de respaldo (cualquier copia de seguridad de configuración almacenada en disk0 o disco duro se perderá como parte del procedimiento de recuperación de contraseña, por lo que siempre guarde la configuración en un servidor externo). Asegúrese de ver este mensaje en los registros de la consola RP0 para RP0 y RP1, como un paso de verificación para confirmar la recuperación de la contraseña y para verificar que toda la limpieza de datos de usuario anterior se haya completado exitosamente para ambos RP. Si no es así, repita el paso de requisito previo y el paso 1. a 4. hasta que vea estos mensajes en los registros de la consola RP0. Si este mensaje no se ve para el RP en espera, debe repetir el Paso de Requisito Previo y

el Paso 1. a 4. para el RP en espera solamente.

```
RP/0/RP0/CPU0:Jul 8 06:13:24.551 CEST: sys_rec[1188]: %SECURITY-SYSTEM_RECOVERY-1-REPORT :  
System Recovery at 06:10:19 CEST Thu Jul 08 2021 was successful
```

```
RP/0/RP1/CPU0:Jul 8 06:15:13.967 CEST: sys_rec[1188]: %SECURITY-SYSTEM_RECOVERY-1-REPORT :  
System Recovery at 06:11:23 CEST Thu Jul 08 2021 was successful
```

Summary

Este nuevo procedimiento de recuperación de contraseña se puede utilizar para restablecer de forma segura las contraseñas perdidas en la plataforma Cisco serie 8000 y la plataforma NCS serie 5500 en menos de 10 minutos.