Resolución de problemas de recuperación de contraseña CIMC para plataformas ENCS

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Pasos de recuperación de contraseña CIMC

Introducción

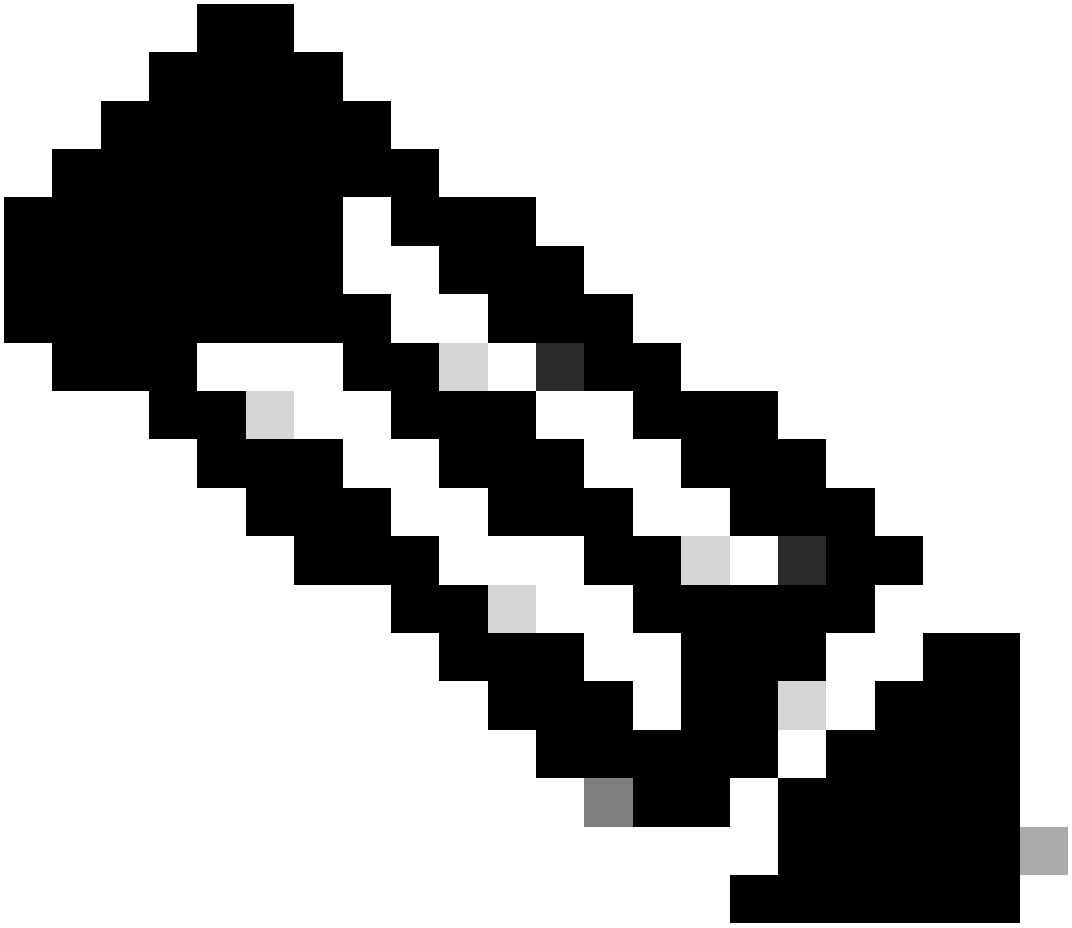
Este documento describe una guía paso a paso sobre cómo recuperar las credenciales CIMC para las plataformas ENCS 54XX que tienen capacidad CIMC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Este documento se aplica a los dispositivos ENCS que tienen capacidad CIMC.
- El proceso puede variar en otras plataformas, como uCPE Catalyst 8300 y módulos CSP, que también cuentan con funciones CIMC.
- Debe tener acceso o disponibilidad de dispositivo físico para administrar de forma remota la fuente de alimentación del dispositivo afectado.
- Para realizar una recuperación de contraseña CIMC, debe tener una conexión de consola CIMC desde el dispositivo. No se puede utilizar una conexión SSH o Telnet con el dispositivo para este proceso.



Nota: Se puede utilizar un servidor Terminal Server para la conexión de consola. Sin embargo, se recomienda la conexión directa a la consola.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Hardware: ENCS5412/K9
- Versión del firmware de CIMC: 3.2(14.19)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Estos pasos se pueden utilizar para recuperar el acceso CIMC restableciendo las credenciales CIMC a sus valores predeterminados.
El propósito principal de este proceso de recuperación de contraseña es eliminar la partición EMMC que tiene la configuración CIMC para borrar las credenciales desconocidas.

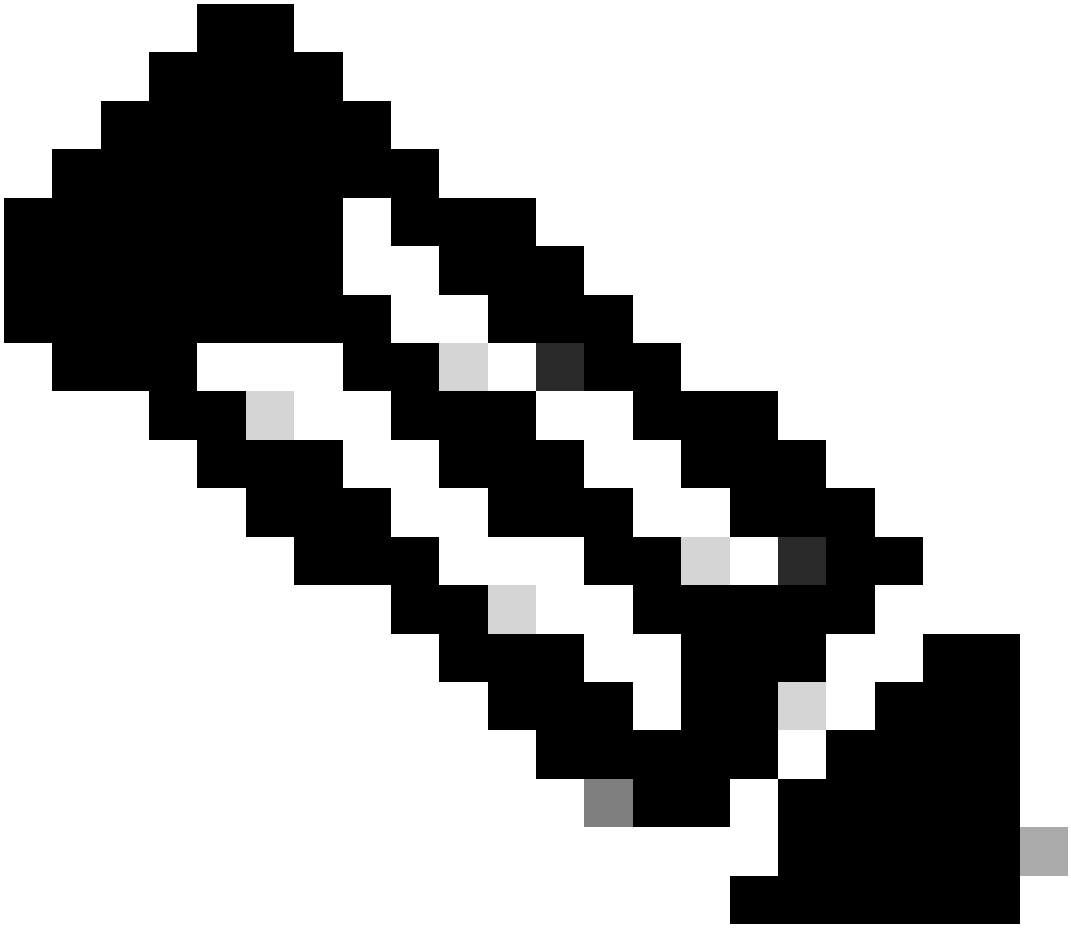
Advertencia: Al formatear la partición EMMC, se borra el contenido de la tarjeta EMMC, como la configuración del controlador de administración de la placa base, el archivo ISO y la contraseña. Realice una copia de seguridad de la VM alojada a través de CIMC antes de continuar con los pasos de recuperación de contraseña.

Pasos de recuperación de contraseña CIMC

Paso 1. Reinicie el dispositivo. Se le pedirá que recargue el dispositivo desde la fuente de

alimentación o que lo desconecte de la fuente de alimentación ya que no tiene acceso al dispositivo.

Paso 2. Mientras el dispositivo se está iniciando, se muestra un mensaje para detener el proceso de arranque automático. Escriba *** para detenerlo.



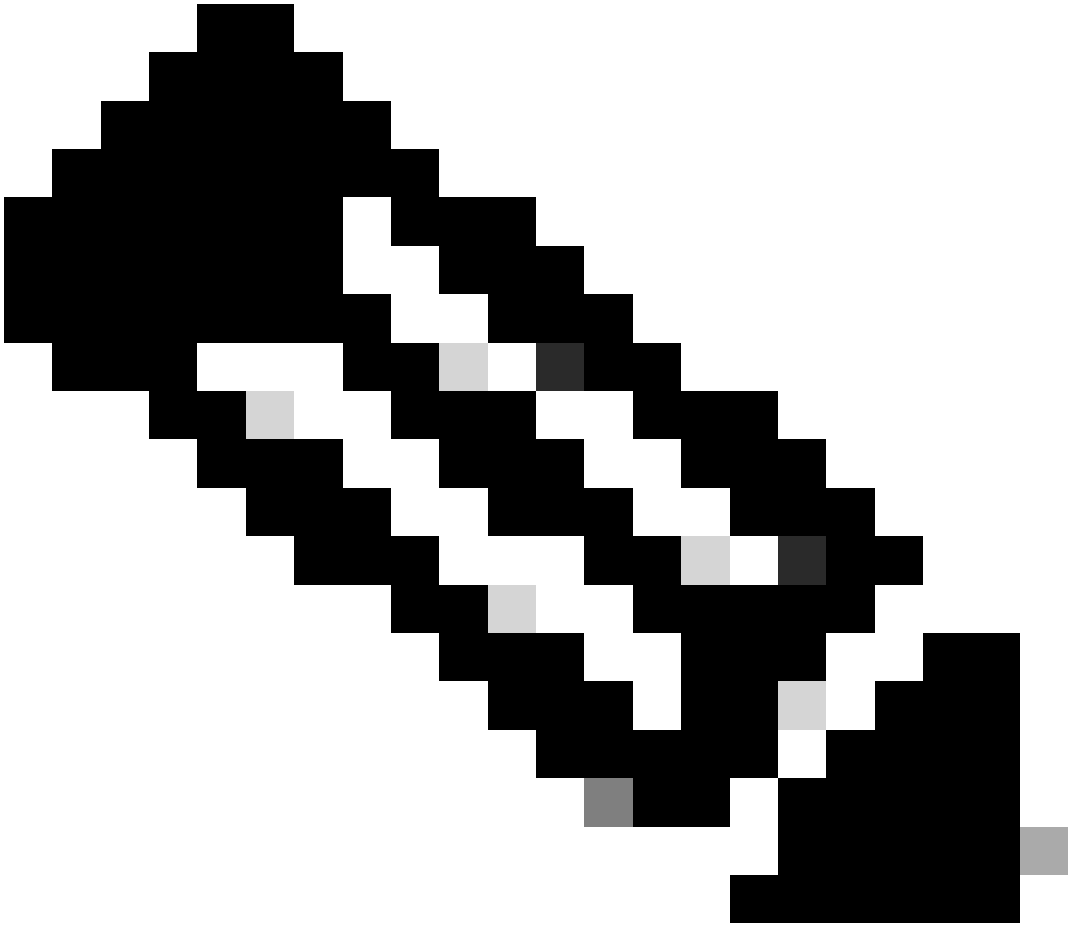
> Nota: Compruebe dónde está el carácter (*) en el teclado antes de comenzar con este proceso. Este paso tiene un tiempo limitado de 10 segundos para ejecutarse.

<#root>

```
CHIMP v1.3
Copyright Cisco Systems, Inc. (c) 2011, 2012

Attempting cisco_chimp_boot with FLAT_MMU algo
Divisor: 0x00000008
Checking if we are already running from PLL
Already running from PLL
Image 1 validation in progress
Image 1 validation COMPLETE
```

```
U-Boot 1.1.4 (Jun 4 2024 - 16:03:59)
U-Boot code: 87F00000 -> 87F21AAC BSS: -> 87F26164
IRQ Stack: 87e9ff7c
FIQ Stack: 87e9ef7c
RAM Configuration:
Bank #0: 80800000 256 MB
Found SPI Chip Numonyx N28Q128
Flash: 16 MB
Using default environment

Net: Phy Id dd1 not matching dev_num is 0
Phy Id ffff not matching dev_num is 1
pilot_eth0, pilot_eth1
Enable port 80 capture.

Type *** to stop autoboot:
```

Paso 3. Cuando se evita el arranque automático, el dispositivo solicita el terminal ucse-cimc. Escriba boot current recovery para iniciar en modo de recuperación.
Paso 4. Una vez que inicie en el modo de recuperación, el dispositivo solicita las credenciales predeterminadas para entrar en el modo de recuperación.



Nota: Las credenciales predeterminadas de CIMC son: admin como nombre de usuario y contraseña como contraseña. El analizador de la línea de comandos recovery-shell es muy primitivo y no puede analizar la tecla de flecha, la tecla de retroceso o la mayoría de los caracteres especiales. Escriba el comando exacto.

<#root>

```
starting pid 1146, tty '': '/sbin/getty -L ttyS0 9600 vt100'

CISCO-IMC login:

admin


Password:

password


login[1146]: root login on 'ttyS0'
recovery-shell#
```

Paso 5. En el mensaje del shell de recuperación, escriba emmc format p3 para formatear la partición p3 en la tarjeta EMMC que tiene la configuración CIMC.

```
<#root>

recovery-shell#

emmc format p3


Formatting partition 3
done
```

Paso 6. Una vez que el proceso de formateo haya terminado, escriba reboot para volver al inicio normal de CIMC. Una vez que CIMC haya arrancado, inicie sesión con las credenciales predeterminadas y continúe con los pasos para crear una nueva contraseña.

```
<#root>

recovery-shell#

reboot


Restarting system.


CHIMP v1.3
Copyright Cisco Systems, Inc. (c) 2011, 2012

Attempting cisco_chimp_boot with FLAT_MMU algo
Divisor: 0x00000008
Checking if we are already running from PLL
Already running from PLL
Image 1 validation in progress
Image 1 validation COMPLETE

<output omitted>

Successfully reset boot order to factory defaults
BMC-LAST-SCRIPT [SUCCESS]
OP:[ on ] OP-CCODE:[ Success ]
OP:[ fp_lock ] OP-CCODE:[ Success ]
ls: /mnt/datastore/*gold*: No such file or directory
starting pid 4670, tty '': '/sbin/getty -L ttyS0 9600 vt100'
ENCS5412-FGL223781BV login:

admin


Password:

password


**********WARNING!**********
```

```
Default credentials were used for login.
Administrator password needs to be
changed for security purposes.
****************************************
Enter current password:
```

password

```
Please change the password...
Enter new password:
```

<

>

```
Re-enter new password:
```

<

>

```
Updating password...
Password updated successfully.
ENCS5412-FGL223781BV#
```

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).