Restablecer la contraseña del usuario administrador en un sistema Firepower

Contenido

kWh

Introducción

Este documento describe los pasos de instrucciones para restablecer la contraseña de la cuenta de administrador en un sistema Firepower.

Antecedentes

Firepower Management Center (FMC) proporciona diferentes cuentas de administración (con contraseñas independientes) para el acceso a la interfaz de línea de comandos (CLI)/shell y el acceso a la interfaz web (cuando esté disponible). La cuenta de administrador de los dispositivos administrados, como Firepower y los dispositivos de servicios Firepower del dispositivo de seguridad adaptable (ASA), es la misma para el acceso CLI, el acceso al shell y el acceso a la interfaz web (cuando estén disponibles).

Estas instrucciones citan al Centro de administración Firepower.

> **Nota**: las referencias a la CLI de Firepower Management Center solo se aplican a las versiones 6.3+. Los dispositivos de las series 7000 y 8000 son compatibles con la versión 6.4.

Firepower Threat Defense: restablezca la contraseña de administrador

Para restablecer una contraseña de administrador perdida para un dispositivo lógico Firepower Threat Defence (FTD) en las plataformas Firepower 9300 y 4100, siga las instrucciones de la guía Cambiar o recuperar contraseña para FTD mediante FXOS Chassis Manager.

Para los dispositivos FTD ejecutados en Firepower 1000/2100/3100, debe recrear la imagen del dispositivo. Consulte la Guía de Troubleshooting de Cisco FXOS para Firepower 1000/2100 Series Running Firepower Threat Defense para ver el Procedimiento de Recreación de Imágenes en estas plataformas.

En el caso de los dispositivos FTD que se ejecuten en los modelos ASA 5500-X y Integrated Security Appliance (ISA) 3000, debe volver a crear una imagen del dispositivo. Consulte la Guía de rediseño de dispositivos Cisco ASA y Firepower Threat Defense para obtener instrucciones.

En el caso de los dispositivos FTD virtuales, debe sustituir el dispositivo por una nueva implementación.

La recreación de imágenes de un dispositivo físico borra su configuración y restablece la contraseña de administración en **Admin123**.

Con la excepción de FTDvs que utilizan Firepower 7.0+ en Amazon Web Services (AWS), una nueva implementación de FTDv no tiene configuraciones y la contraseña de administración es **Admin123**. Para FTDvs que utilizan Firepower 7.0+ en AWS, una nueva implementación no tiene configuración y no hay contraseña predeterminada; debe proporcionar una contraseña de administrador en el momento de la implementación.

- Si vuelve a crear una imagen de un dispositivo FTD administrado con el administrador de dispositivos Firepower:
  - Si dispone de una copia de seguridad reciente almacenada externamente, puede restaurar las configuraciones de la copia de seguridad después de volver a crear la imagen. Para obtener más información, consulte la Guía de configuración de Cisco Firepower Threat Defense para Firepower Device Manager.para obtener su versión.
  - Si no dispone de una copia de seguridad, debe volver a crear la configuración del dispositivo manualmente, que incluye las interfaces, las directivas de enrutamiento y los parámetros de DHCP y del sistema dinámico de nombres de dominio (DDNS).
- Si vuelve a crear imágenes de un dispositivo FTD gestionado con Firepower Management Center, y el FMC y el dispositivo que ejecuta la versión 6.3+, puede utilizar la interfaz web de FMC para realizar una copia de seguridad de la configuración del dispositivo antes de volver a crear la imagen y restaurar la copia de seguridad después de volver a crear la imagen. Para obtener más información, consulte la Guía de configuración del Centro de administración Firepower correspondiente a su versión.

> **Nota**: Si ejecuta la versión 6.0.1-6.2.3, no podrá realizar una copia de seguridad de la configuración de FTD. Si ejecuta la versión 6.3.0 - 6.6.0, las copias de seguridad y la restauración desde la interfaz web de FMC no se admiten para las instancias de contenedores de FTD. Aunque puede aplicar políticas compartidas desde Firepower Management Center después de volver a crear la imagen, debe configurar manualmente cualquier parámetro específico del dispositivo, como la interfaz, las políticas de routing y los parámetros DHCP y DDNS.

Módulo ASA Firepower Services: restablecimiento de la contraseña de administrador

Puede restablecer la contraseña de administración de la CLI del módulo ASA Firepower con el comando session de la CLI de operaciones generales de ASA. Si ha perdido las contraseñas de la CLI de ASA, puede

recuperarlas tal y como se describe en la Guía de configuración de CLI Book 1: Cisco ASA Series General Operations para su versión de ASA.

Restablezca la contraseña de administrador en los dispositivos ASA 5512-X, ASA 5555-X y ASA 5506-X, ASA 5516-X (módulo de potencia de fuego de software ASA) e ISA 3000

Para restablecer el usuario administrador del módulo de software ASA Firepower o el dispositivo ISA 3000 a la contraseña predeterminada, ingrese este comando en el indicador de ASA:

```
session sfr do password-reset
```

Para obtener más información, consulte la Guía de configuración de la CLI Book 2 de Cisco ASA Series: Firewall de Cisco ASA para su versión de ASA.

Restablecer la contraseña de administrador en los dispositivos ASA serie 5585-X (módulo Firepower de hardware ASA)

Para restablecer el usuario administrador del módulo de hardware ASA FirePOWER a la contraseña predeterminada, introduzca este comando en el indicador de ASA:

```
session 1 do password-reset
```

Para obtener más información, consulte la Guía de configuración de la CLI Book 2 de Cisco ASA Series: Firewall de Cisco ASA para su versión de ASA.

Cambiar la contraseña de administración de CLI o Shell para FMCs y NGIPSv

Siga estas instrucciones para restablecer una contraseña conocida para estas cuentas de administrador:

- Firepower Management Center: contraseña de administrador utilizada para acceder a la CLI o al shell.
- Next Generation Information Preservation System virtual (NGIPSv): contraseña de administrador utilizada para acceder a la CLI.

Procedimiento:

1. Inicie sesión en la cuenta de administrador del dispositivo mediante SSH o la consola.
    - Para Firepower Management Center:
        - Si Firepower Management Center ejecuta Firepower versión 6.2 o inferior, el inicio de sesión le proporcionará acceso directo al shell de Linux.
        - Si Firepower Management Center ejecuta Firepower versión 6.3 o 6.4 y la CLI de Firepower Management Center no está habilitada, el inicio de sesión le proporciona acceso directo al shell de Linux.
        - Si Firepower Management Center ejecuta Firepower versión 6.3 o 6.4 y la CLI de Firepower Management está activada, el inicio de sesión le dará acceso a la CLI de Firepower Management Center. Ingrese el comando expert para acceder al shell de Linux.
        - Si Firepower Management Center ejecuta Firepower versión 6.5+, el inicio de sesión le dará acceso a la CLI de Firepower Management Center. Ingrese el comando expert para acceder al shell de Linux.
    - En el caso de los dispositivos gestionados, el inicio de sesión le proporciona acceso a la CLI del dispositivo. Ingrese el comando expert para acceder al shell de Linux.

2. En el indicador de shell, ingrese este comando: **sudo passwd admin**.
3. Cuando se le solicite, ingrese la contraseña de administrador actual para elevar el privilegio al acceso raíz.
4. En respuesta a las solicitudes, ingrese la nueva contraseña de administrador dos veces.

> **Nota**: Si el sistema muestra un BAD PASSWORD mensaje, esto es sólo informativo. El sistema aplica la contraseña que proporciona incluso si aparece este mensaje. Sin embargo, Cisco recomienda que utilice una contraseña más compleja por motivos de seguridad.

---

5. Tipo exit para salir del shell.
6. En un dispositivo administrado o en un FirePOWER Management Center con la CLI habilitada, escriba exit para salir de la CLI.

Cambie la contraseña de administración de la interfaz web para los FMC o la contraseña de administración de la interfaz web y la contraseña de administración de la CLI para los dispositivos de las series 7000 y 8000

Siga estas instrucciones para restablecer una contraseña conocida para estas cuentas de administrador:

- Firepower Management Center: contraseña de administrador utilizada para acceder a la interfaz web.
- Dispositivos de las series 7000 y 8000: contraseña de administración utilizada para acceder a la interfaz web, así como a la CLI.

Procedimiento:

1. Inicie sesión en la interfaz web del dispositivo como usuario con acceso de administrador.
2. Elegir **System** > **Users** y haga clic en el Edit para el usuario administrador.
3. Introduzca valores para el **Password** y **Confirm Password** campos.
   Los valores deben ser los mismos y deben ajustarse a las opciones de contraseña establecidas para el usuario.
4. Haga clic en Save.

Restablecer una contraseña de administración de shell o CLI perdida para FMCs o NGIPSv, o bien Restablecer una interfaz web perdida o una contraseña de CLI para dispositivos de las series 7000 y 8000

Utilice estas instrucciones para restablecer una contraseña perdida para estas cuentas de administrador:

- Firepower Management Center: contraseña de administrador utilizada para acceder a la CLI o al shell.
- Dispositivos de las series 7000 y 8000: contraseña de administración utilizada para acceder a la interfaz web, así como a la CLI.
- NGIPSv: contraseña de administrador utilizada para acceder a la CLI.

> **Nota**: para restablecer una contraseña perdida para estas cuentas de administrador, debe establecer una conexión de consola o SSH con el dispositivo (en el caso de un Firepower Management Center con usuarios externos configurados, puede utilizar una conexión SSH). También debe reiniciar el dispositivo cuyas credenciales de administrador perdió. Puede iniciar el reinicio de diferentes

---

maneras, dependiendo del tipo de acceso del dispositivo que tenga disponible:
· Para Firepower Management Center, necesita las credenciales de inicio de sesión de un usuario de interfaz web con acceso de administrador o las credenciales de inicio de sesión de un usuario autenticado externamente con acceso CLI/shell.
· Para los dispositivos de las series 7000 u 8000, necesita las credenciales de inicio de sesión para uno de estos medios de acceso: un usuario de interfaz web con acceso de administrador, un usuario de CLI con acceso de configuración o un usuario con acceso de administrador en el Firepower Management Center administrado.
· Para NGIPSv, necesita credenciales de inicio de sesión para un usuario de CLI con acceso a configuración o un usuario con acceso de administrador en el Firepower Management Center administrado.
· En el caso de los dispositivos Firepower Management Center de las series 7000 y 8000 y los dispositivos NGIPSv, si dispone de una conexión de consola (física o remota), puede realizar esta tarea sin credenciales de inicio de sesión.
Si no puede acceder al dispositivo con uno de estos métodos, no puede restablecer la contraseña de administrador con estas instrucciones. Póngase en contacto con el TAC de Cisco.

Opción 1. Reinicie de forma segura el dispositivo e ingrese el modo de usuario único en el arranque para restablecer la contraseña

1. Abra una conexión a la consola del dispositivo para el dispositivo cuya contraseña de administrador perdió:
   · Para los dispositivos de la serie 7000, los dispositivos de la serie 8000 y los Firepower Management Centers, utilice una conexión de teclado/monitor o serie.
   · Para los appliances virtuales, utilice la consola proporcionada por la plataforma virtual. Consulte la Guía de inicio virtual de Cisco Firepower Management Center o la Guía de inicio rápido de Cisco Firepower NGIPSv para VMware para obtener más información.
   · Como alternativa, para Firepower Management Centers, series 7000 y 8000, y appliances virtuales, si tiene una conexión de consola establecida con el appliance mediante el uso del teclado, vídeo y ratón (KVM) remoto, puede acceder a esa interfaz.
2. Reinicie el dispositivo cuya contraseña de administrador perdió. Tiene estas opciones:
   â€¢ Para el Centro de administración Firepower:
   a. Inicie sesión en la interfaz web del Centro de administración Firepower como usuario con acceso de administrador.
   b. Reinicie el Centro de administración Firepower como se describe en la Guía de configuración del Centro de administración Firepower para su versión.

   · Para dispositivos de las series 7000 u 8000 o NGIPSv, si dispone de credenciales para un usuario de interfaz web con acceso de administrador en el Firepower Management Center administrado:
   a. Inicie sesión en la interfaz web del Firepower Management Center gestionado como un usuario con acceso de administrador.
   b. Apague y reinicie el dispositivo administrado como se describe en la Guía de configuración del Centro de administración Firepower para su versión.

   â€¢ Para los dispositivos de las series 7000 u 8000, si tiene credenciales para un usuario de interfaz web con acceso de administrador:
   a. Inicie sesión en la interfaz web del dispositivo como usuario con acceso de administrador.
   b. Reinicie el dispositivo como se describe en la Guía de configuración del Centro de administración Firepower para su versión.

   â€¢ Para dispositivos de las series 7000 u 8000 o NGIPSv, si tiene credenciales para un usuario de la CLI con acceso de configuración:

a. Inicie sesión en el dispositivo mediante el shell a través de un nombre de usuario con acceso a la configuración CLI.
b. En la línea de comandos, escriba el comando system reboot.

· Para Firepower Management Centers, series 7000 y 8000 y appliances virtuales con consola, pulse CTRL-ALT-DEL. (Si utiliza un KVM remoto, la interfaz KVM proporciona una forma de enviar **CTRL-ALT-DEL** al dispositivo sin interferencias con el propio KVM.)

Nota: cuando se reinicia Firepower Management Center o un dispositivo gestionado, se cierra la sesión del dispositivo y el sistema ejecuta una comprobación de la base de datos que puede tardar hasta una hora en completarse.

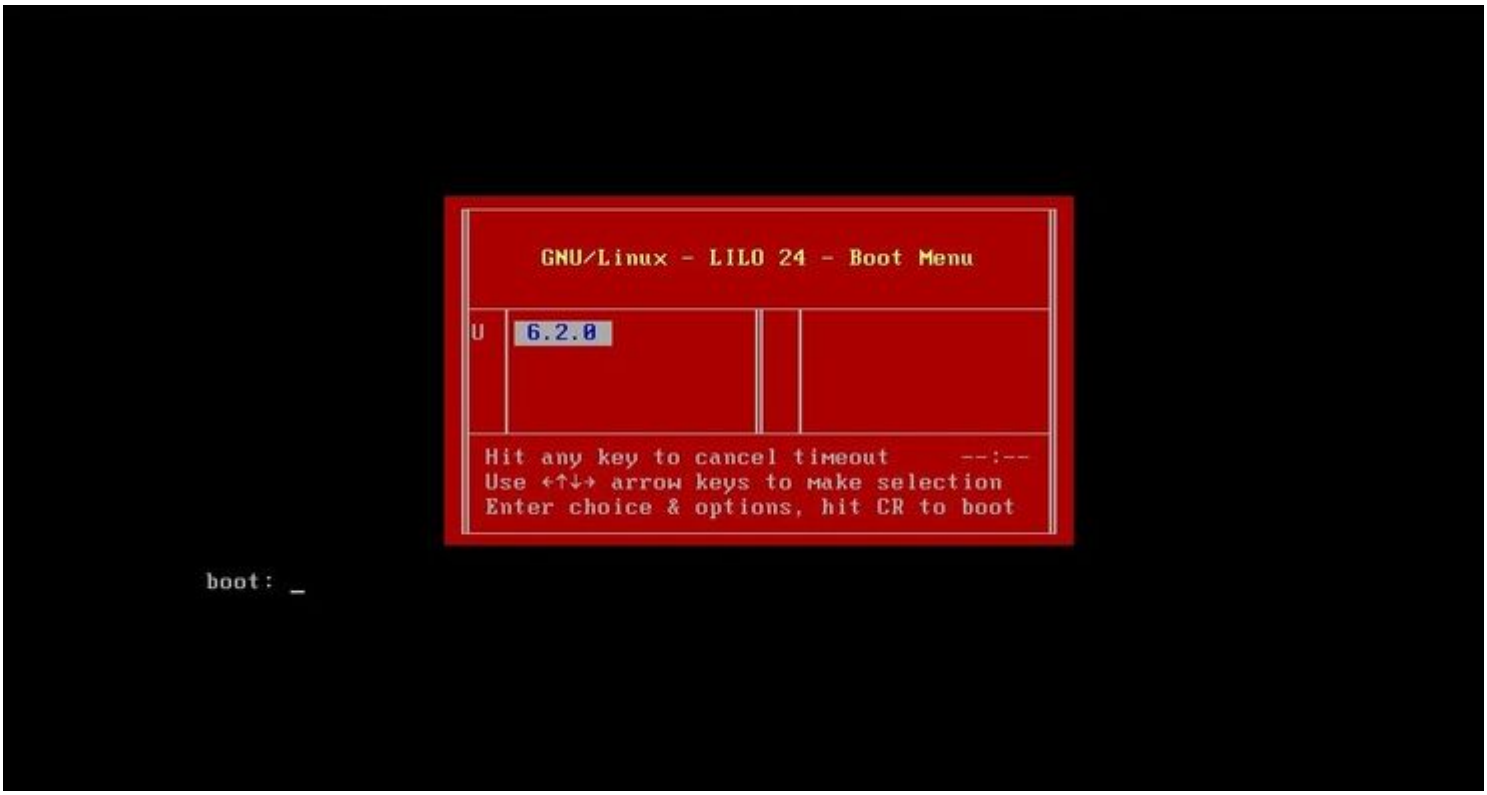
Precaución: no apague los dispositivos con el botón de encendido ni desenchufe el cable de alimentación, ya que podría dañar la base de datos del sistema. Cierre los dispositivos completamente mediante la interfaz web.

---

3. En la pantalla de la consola del equipo, observe el proceso de reinicio y continúe dependiendo del tipo de equipo que se reinicie:

Nota: Si el sistema está en proceso de comprobación de la base de datos, puede ver el mensaje: The system is not operational yet. Checking and repairing the database is in progress. This may take a long time to finish**.**

â€¢ Para los modelos de Centros de administración Firepower 750, 1500, 2000, 3500 o 4000, o para dispositivos Firepower de las series 7000 u 8000 o NGIPSv, interrumpa el proceso de reinicio:
a. Una vez que el dispositivo comienza a arrancar, presione cualquier tecla del teclado para cancelar la cuenta regresiva en el menú de arranque de LILO.
b. Observe el número de versión que se muestra en el menú de arranque de LILO. En este ejemplo, el número de versión es 6.2.0.



c. En el indicador boot:, escriba el comando version single donde version es el número de versión (por ejemplo 6.2.0 single). Si el sistema tiene activada la compatibilidad con la lista de productos aprobados de capacidades unificadas (UCAPL), se le solicitará una contraseña; introduzca la contraseña **Sourcefire**.

· Para los modelos 1000, 1600, 2500, 2600, 4500 o 4600 de Firepower Management Centers:
Cuando aparezca el menú de arranque, seleccione Option 4, Cisco Firepower Management Console Password Restore Mode.

4. Asigne una nueva contraseña de administrador; siga las instrucciones correspondientes a su dispositivo:
· Para obtener una nueva contraseña de administración de shell y CLI para Firepower Management Center o NGIPSv:

a. Cuando el sistema muestre un mensaje del sistema operativo que termine con un signo de almohadilla (#), ingrese este comando:

```
passwd admin
```

b. Introduzca la nueva contraseña de administrador cuando se le solicite hacerlo (dos veces).

Nota: Si el sistema muestra un BAD PASSWORD mensaje, esto es sólo informativo. El sistema aplica la contraseña que proporciona incluso si aparece este mensaje. Sin embargo, se recomienda utilizar una contraseña más compleja por motivos de seguridad.

· Para obtener una nueva contraseña de administración de Web y CLI para los dispositivos de las series 7000 y 8000:

En el indicador del sistema operativo que termina con el signo de almohadilla (#), ingrese este comando:

```
usertool.pl -p 'admin password'
```

Donde una contraseña es la nueva contraseña de administrador.

5. Si la cuenta de administrador se ha bloqueado debido a demasiados intentos fallidos de inicio de sesión, debe desbloquearla. Siga las instrucciones correspondientes a su dispositivo:

· Para desbloquear las cuentas de administración de CLI y shell en un Firepower Management Center o NGIPSv, introduzca este comando en el indicador del sistema operativo que termina con el signo de almohadilla (#):

```
pam_tally --user admin --reset
```

· Para desbloquear las cuentas de administración Web y CLI en los dispositivos de las series 7000 y 8000, ingrese este comando en el indicador del sistema operativo que termina con un signo de almohadilla (#):

```
usertool.pl -u admin
```

6. En el indicador del sistema operativo que termina con el signo de almohadilla (#), introduzca el reboot comando.

7. Deje que finalice el proceso de reinicio.

Opción 2. Utilizar la autenticación externa para obtener acceso a la CLI para restablecer la contraseña de un FirePOWER Management Center

Si se encuentra en una situación en la que todavía tiene acceso a la interfaz web de FMC con una cuenta con acceso de administrador, puede utilizar el External Authentication para obtener acceso a la CLI. Este método le permite iniciar sesión en la CLI de un FMC, acceder al shell de Linux, elevarse a root y restablecer la contraseña de administración de CLI/shell manualmente. Esta opción no requiere reinicio ni acceso a la consola. Esta opción requiere que haya configurado correctamente la autenticación externa (con acceso SSH) en Firepower Management Center para el que desea restablecer la contraseña de administrador. (Consulte la Guía de configuración de Firepower Management Center para obtener información sobre su versión). Una vez configurado, siga estos pasos:

1. Inicie sesión en Firepower Management Center con una cuenta autenticada externamente que tenga acceso CLI/shell con el uso de SSH o la consola:
   · Si su FMC ejecuta la versión 6.2 o inferior, esto le da acceso directo al shell de Linux.
   · Si su FMC ejecuta la versión 6.3 o 6.4 y la CLI de FMC no está habilitada, esto le da acceso directo al shell de Linux.
   · Si el FMC ejecuta la versión 6.3 o 6.4 y la CLI de Firepower Management Center está habilitada, esto le dará acceso a la CLI de Firepower Management Center. Escriba el expert para acceder al shell de Linux.
   · Si su FMC ejecuta la versión 6.5+, esto le dará acceso a la CLI de Firepower Management Center. Escriba el **expert** para acceder al shell de Linux.
2. En el indicador de shell con un símbolo de dólar ($), ingrese este comando para restablecer la contraseña de CLI para el usuario administrador:
   sudo passwd admin
3. En el Password prompt, ingrese la contraseña para el nombre de usuario con el que inició sesión actualmente.
4. Introduzca la nueva contraseña de administrador cuando se le solicite hacerlo (dos veces).

> **Nota**: Si el sistema muestra un mensaje **CONTRASEÑA ERRÓNEA**, es sólo informativo. El sistema aplicará la contraseña que proporcione, incluso si aparece este mensaje. Sin embargo, Cisco recomienda que utilice una contraseña más compleja por motivos de seguridad.

---

5. Si se ha bloqueado la cuenta **admin** debido a demasiados intentos fallidos de inicio de sesión, debe desbloquear la cuenta y ejecutar el pam_tally e introduzca la contraseña cuando se le solicite:
   sudo pam_tally --user --reset
6. Tipo exit para salir del shell.
7. En un Firepower Management Center con la CLI habilitada, escriba **exit** para salir de la CLI.

Restablecer una contraseña de administrador de interfaz web perdida para Firepower Management Centers

Siga estas instrucciones para cambiar la contraseña de la cuenta de administrador utilizada para acceder a la interfaz web de Firepower Management Center.

Procedimiento:

1. Inicie sesión en el dispositivo con la cuenta de administrador de CLI con SSH o la consola.
2. Acceda al shell de Linux:
   · Si su FMC ejecuta la versión 6.2 o inferior, el inicio de sesión le da acceso directo al shell de Linux.
   · Si el FMC ejecuta la versión 6.3 o 6.4 y la CLI de Firepower Management Center no está habilitada, el inicio de sesión le proporciona acceso directo al shell de Linux.
   · Si el FMC ejecuta la versión 6.3 o 6.4 y la CLI de Firepower Management Center está activada, el inicio de sesión le dará acceso a la CLI de Firepower Management Center. Escriba el expert para acceder al shell de Linux.
   · Si su FMC ejecuta la versión 6.5+, el inicio de sesión le dará acceso a la CLI de Firepower

Management Center. Escriba el **expert** para acceder al shell de Linux.

3. En la indicación del shell, ingrese este comando para restablecer la contraseña para el usuario administrador de la interfaz web:

   sudo usertool.pl -p 'admin password'

   Donde **password** es la nueva contraseña para el usuario administrador de la interfaz web.
4. En el **Password** prompt, ingrese la contraseña para el nombre de usuario con el que inició sesión actualmente.
5. Si la cuenta de administrador web se ha bloqueado debido a demasiados intentos fallidos de inicio de sesión, debe desbloquearla. Ejecute el usertool , ingrese su contraseña de administrador de CLI cuando se le solicite:

   sudo usertool.pl -u admin
6. Tipo exit para salir del shell.
7. En un Firepower Management Center con la CLI habilitada, escriba exit para salir de la 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).