

Cambio de las credenciales de los dispositivos de Cisco Catalyst Center para dispositivos por cable e inalámbricos en situaciones de red SDA y no SDA

Contenido

[Introducción](#)

[Antecedentes](#)

[Sinopsis](#)

[Solución \(Prácticas recomendadas\)](#)

[Requirements](#)

[Requisitos previos](#)

[Procedimiento para el cambio de credenciales desde Cisco Catalyst Center](#)

[Sitios con AAA gestionada de Cisco Catalyst Center](#)

[El requisito es cambiar la contraseña del usuario \(no cambiar la contraseña de activación\)](#)

[El requisito es cambiar la contraseña del usuario y la contraseña de activación](#)

[Sitios con AAA no administrada de Cisco Catalyst Center](#)

[El requisito es cambiar la contraseña del usuario \(no cambiar la contraseña de activación\)](#)

[El requisito es cambiar la contraseña del usuario y la contraseña de activación](#)

Introducción

En este documento se describen los pasos del procedimiento de cambio de credenciales de Cisco Catalyst Center (anteriormente Cisco DNA Center) para dispositivos con cable e inalámbricos en entornos de red tanto de fabric como no de fabric.

Antecedentes

Este documento también se aplica a sitios con Dynamic Network Access Control (Cisco Catalyst Center) administrado o no administrado Authentication, Authorization and Accounting (AAA).

Sinopsis

Este documento describe la situación en la que existe un requisito de red de actualizar las credenciales utilizadas por Cisco Catalyst Center para la automatización. Cisco Catalyst Center detecta los dispositivos administrados con un nombre de usuario y una contraseña, y Cisco Catalyst Center utiliza esas mismas credenciales para las conexiones SSH a los dispositivos administrados (para la recopilación de inventario/automatización, etc.). Este documento describe las prácticas recomendadas para cambiar la contraseña de los dispositivos administrados

después de que Cisco Catalyst Center los descubra.

Solución (Prácticas recomendadas)

Requirements

1. Para sitios con AAA gestionado por Cisco Catalyst Center

- El requisito es cambiar la contraseña del usuario (no cambiar la contraseña de activación).
- El requisito es cambiar la contraseña del usuario y la contraseña de activación.

2. Para sitios con AAA no gestionado de Cisco Catalyst Center

- El requisito es cambiar la contraseña del usuario (no cambiar la contraseña de activación).
- El requisito es cambiar la contraseña del usuario y la contraseña de activación.

Requisitos previos

- Asegúrese de que AAA no esté configurado en Cisco Catalyst Center para todos los sitios que no sean SDA.
- Utilice un script Python para validar si todos los switches Catalyst 9k (SDA o no SDA) utilizan RADIUS a ISE para los inicios de sesión SSH en las líneas VTY. Corrija los dispositivos que utilizan credenciales locales.
- Para nodos extendidos
 - Para actualizar las líneas vty 0 a 4, utilice estos comandos de configuración (este puede ser el primer paso para los nodos extendidos).

```
line vty 0 4
authorization exec VTY_author
login authentication VTY_authen
```

Procedimiento para el cambio de credenciales desde Cisco Catalyst Center

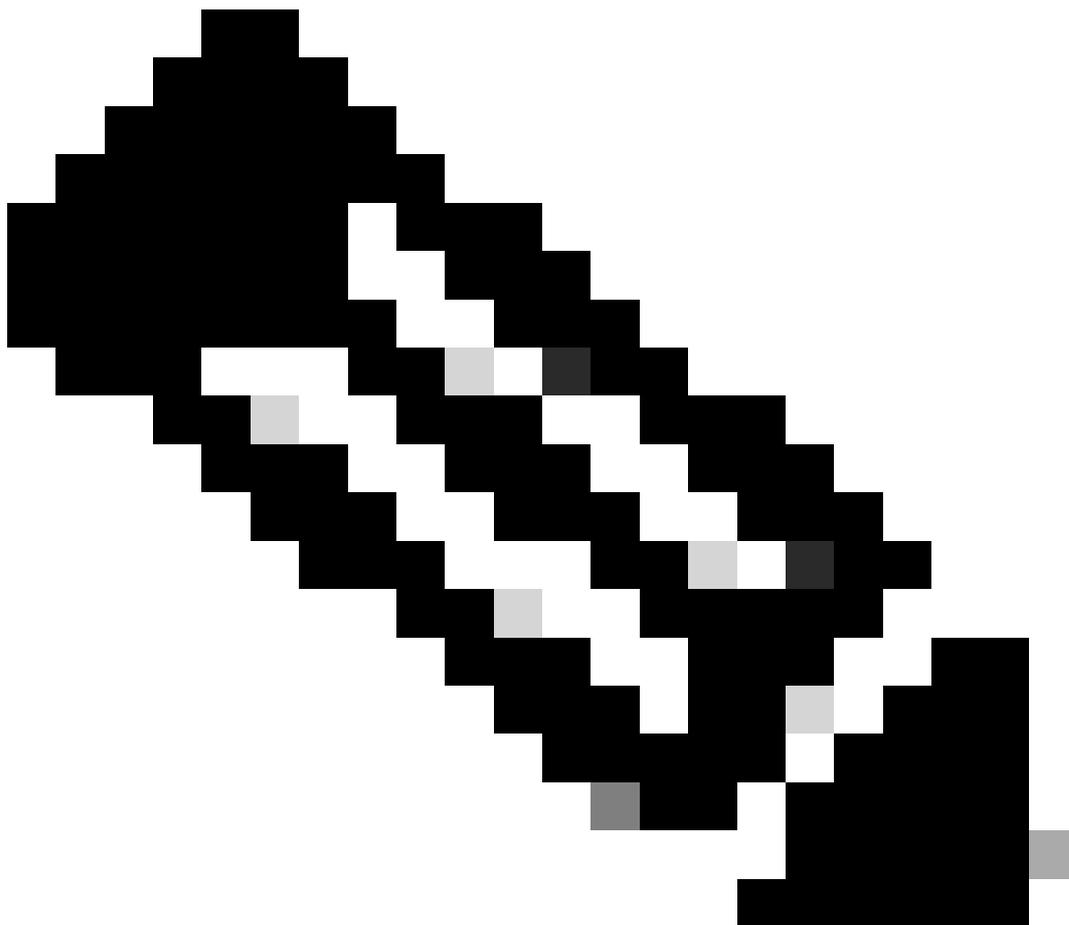
Sitios con AAA gestionada de Cisco Catalyst Center

El requisito es cambiar la contraseña del usuario (no cambiar la contraseña de activación)

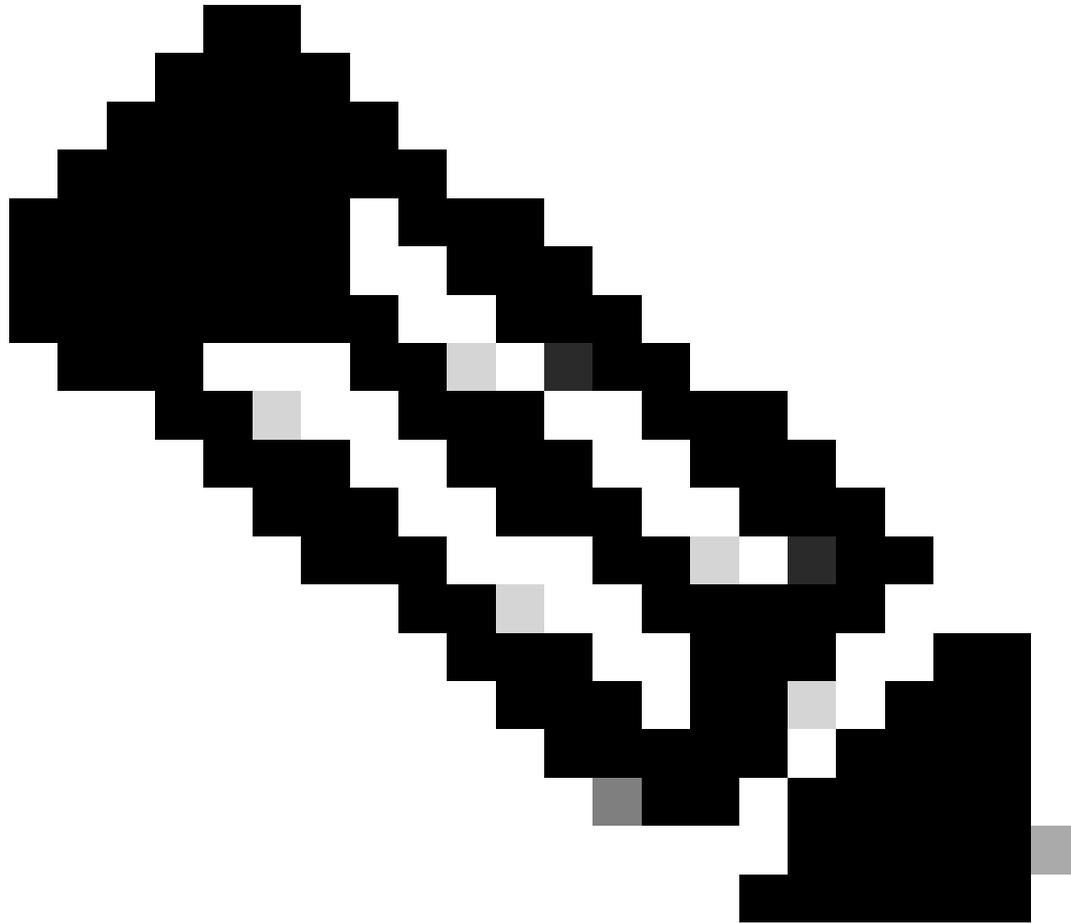
1. En primer lugar, actualice las credenciales (contraseña para el nombre de usuario correspondiente) en ISE. Esto provocará un fallo en la recopilación de inventario y los estados del inventario de dispositivos gestionados cambiarán a Inalcanzable, Fallo de recopilación parcial o Credenciales erróneas.
2. En la página Provisionamiento > Inventario, seleccione uno o varios dispositivos y

seleccione Acciones > Inventario > Editar dispositivo > ficha Credenciales. A continuación, actualice "Add device specific credential" (Agregar credencial específica de dispositivo) con el nuevo nombre de usuario o contraseña (mantenga la misma contraseña de habilitación). Llegados a este punto, Cisco Catalyst Center podrá iniciar sesión en los dispositivos con las credenciales actualizadas y los estados del inventario de dispositivos volverán a Managed (Gestionado).

3. Las credenciales locales de los dispositivos se pueden actualizar como reserva para garantizar que Cisco Catalyst Center pueda iniciar sesión en los dispositivos cuando el servidor AAA externo no esté disponible. Las credenciales locales se pueden actualizar mediante el editor de plantillas de Cisco Catalyst Center, un script personalizado de Python o manualmente.
4. El último paso consiste en actualizar las mismas credenciales en la página Credenciales globales. Esto garantiza que los dispositivos recién descubiertos o los dispositivos que se agregan utilizarán las credenciales actualizadas de la página Diseño > Configuración de red > Credenciales de dispositivo > Credenciales de CLI > editar el nombre de usuario > actualizar la contraseña del usuario sin cambiar la contraseña de habilitación.



Nota: El login SSH/Telnet es autenticado por el servidor AAA externo. Las credenciales del dispositivo local no se actualizan.



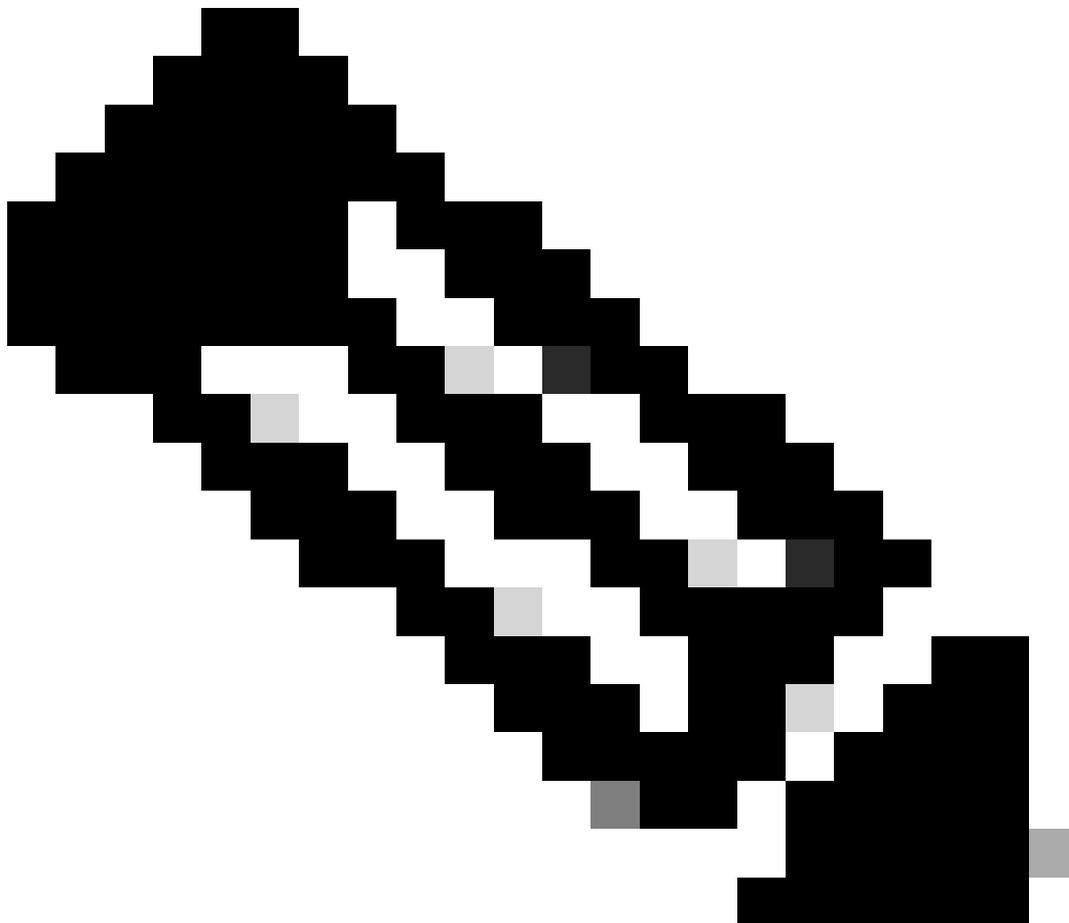
Nota: Cuando se configura un servidor AAA externo en la página de diseño de Cisco Catalyst Center para un sitio, Cisco Catalyst Center no realiza ninguna acción en los dispositivos administrados o ISE cuando se cambian o modifican las credenciales en la página de credenciales globales.

El requisito es cambiar la contraseña del usuario y la contraseña de activación

1. En primer lugar, actualice las credenciales (contraseña para el nombre de usuario correspondiente) en ISE. Esto provocará un fallo en la recopilación de inventario y los estados del inventario de dispositivos gestionados cambiarán a Inalcanzable, Fallo de recopilación parcial o Credenciales erróneas.
2. En la página Provisionamiento > Inventario, seleccione uno o varios dispositivos y

seleccione Acciones > Inventario > Editar dispositivo > ficha Credenciales. A continuación, actualice "Add device specific credential" (Agregar credencial específica de dispositivo) con el nuevo nombre de usuario o contraseña, así como la contraseña de habilitación. Llegados a este punto, Cisco Catalyst Center podrá iniciar sesión en los dispositivos con las credenciales actualizadas y los estados del inventario de dispositivos volverán a Managed (Gestionado).

3. El último paso consiste en actualizar las mismas credenciales en la página Credenciales globales. Esto garantiza que los dispositivos recién descubiertos o los dispositivos que se agregan que mediante la automatización de LAN utilizarán las credenciales actualizadas de la página Diseño > Configuración de red > Credenciales de dispositivo > Credenciales de CLI > editar el nombre de usuario > actualizar la contraseña del usuario y la contraseña de habilitación.



Nota: Cuando el servidor AAA externo es accesible, el nombre de usuario y la contraseña son autenticados por el servidor AAA externo y la contraseña de habilitación es autenticada localmente por el dispositivo administrado.



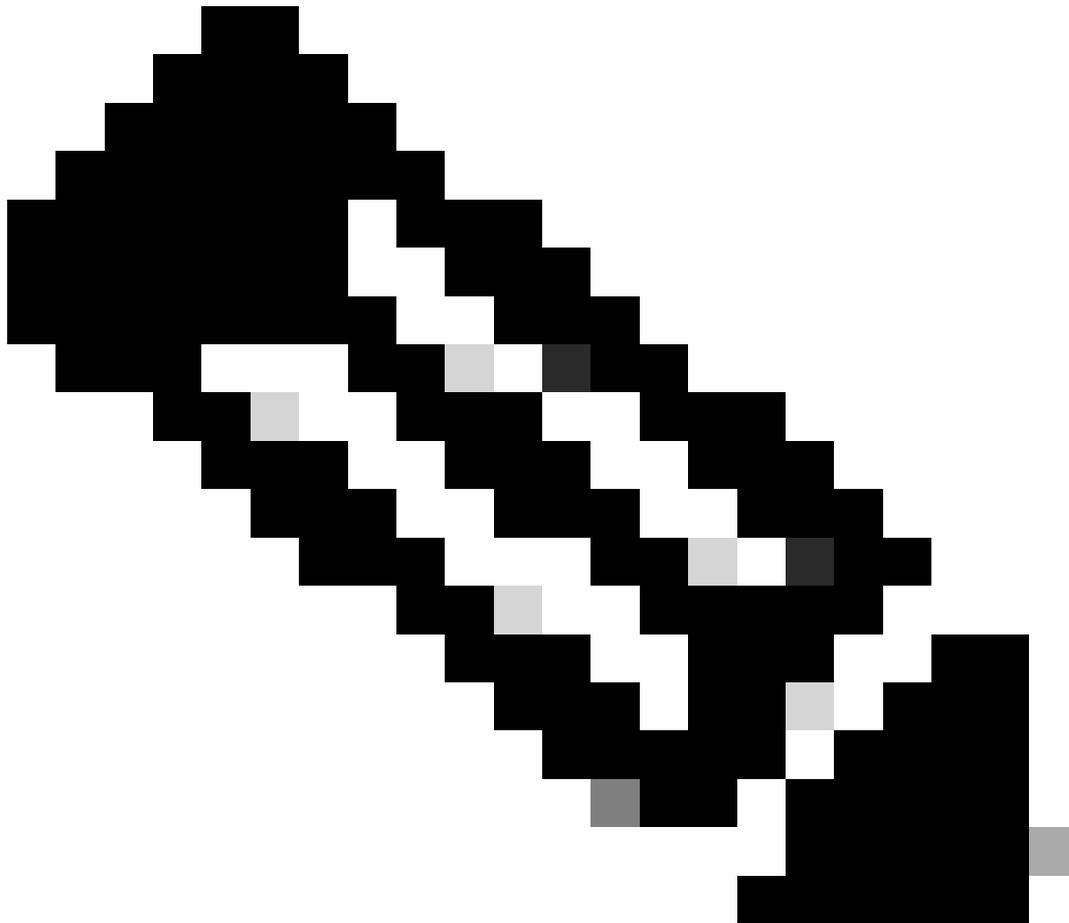
Nota: Cuando se configura un servidor AAA externo en la página de diseño de Cisco Catalyst Center para un sitio, Cisco Catalyst Center no realiza ninguna acción en los dispositivos o ISE cuando se cambian o modifican las credenciales en la página de credenciales globales.

Sitios con AAA no administrada de Cisco Catalyst Center

El requisito es cambiar la contraseña del usuario (no cambiar la contraseña de activación)

1. Actualice las credenciales en la página Credenciales globales en Diseño > Configuración de red > Credenciales de dispositivo > Credenciales de CLI > edite el nombre de usuario > actualice la contraseña del usuario sin cambiar la contraseña de activación.
2. Una vez modificadas las credenciales en la página Credenciales globales, los dispositivos gestionados en los sitios en los que Cisco Catalyst Center no gestiona la AAA se pueden volver a configurar con las credenciales actualizadas. Cisco Catalyst Center puede insertar un script EEM temporal para validar las credenciales. Si el inicio de sesión se realiza

correctamente, la configuración se puede conservar.

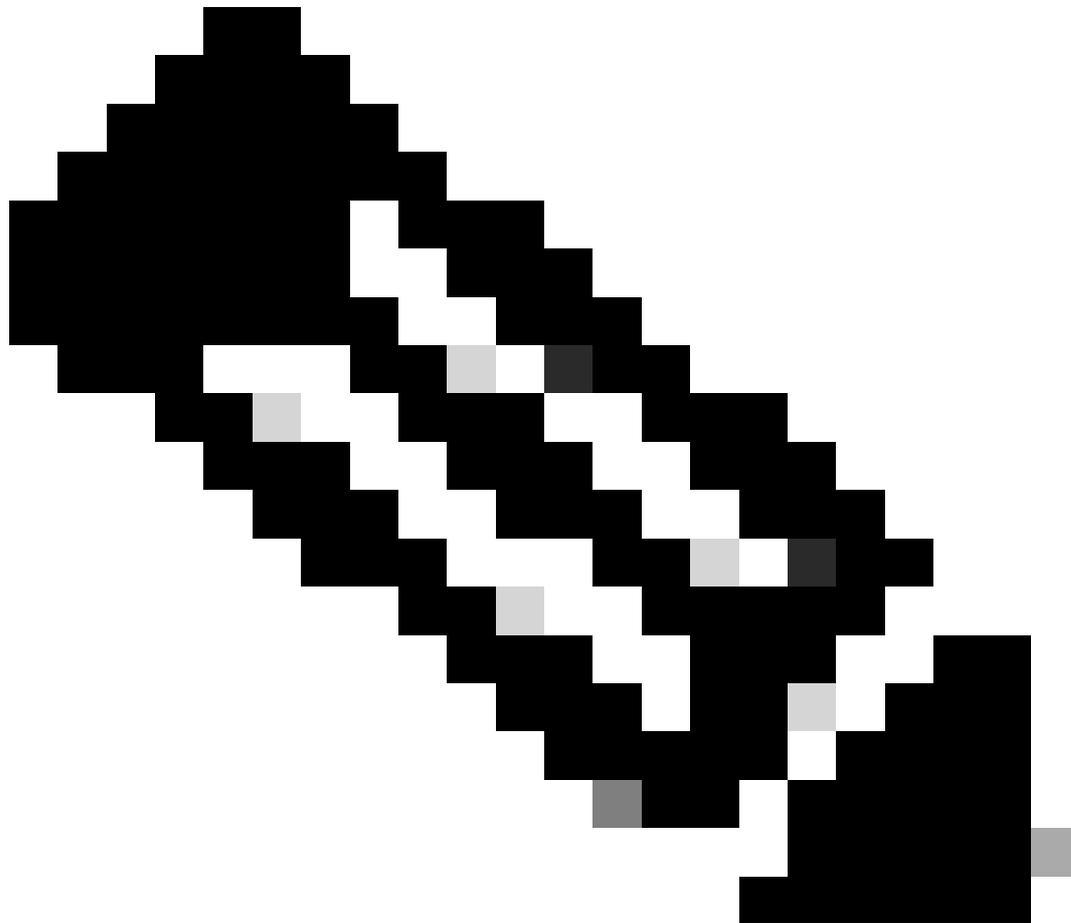


Nota: Para los dispositivos gestionados en los sitios en los que Cisco Catalyst Center no gestiona la configuración AAA, Cisco Catalyst Center no tiene ningún conocimiento sobre si los dispositivos gestionados se configuran manualmente con el servidor AAA externo o si los dispositivos gestionados utilizan solo credenciales locales, de modo que asegúrese de que la contraseña se actualiza en el servidor AAA externo si se configura en los dispositivos gestionados afectados antes de continuar con estos pasos.

El requisito es cambiar la contraseña del usuario y la contraseña de activación

1. Actualice las credenciales en la página Credenciales globales en Diseño > Configuración de red > Credenciales de dispositivo > Credenciales de CLI > edite el nombre de usuario > actualice la contraseña del usuario junto con la contraseña de activación.
2. Una vez modificadas las credenciales en la página Credenciales globales, los dispositivos gestionados en los sitios en los que Cisco Catalyst Center no gestiona la AAA se pueden volver a configurar con las credenciales actualizadas. Cisco Catalyst Center puede insertar

un script EEM temporal para validar las credenciales. Si el inicio de sesión se realiza correctamente, la configuración se puede conservar.



Nota: Para los dispositivos gestionados en los sitios en los que Cisco Catalyst Center no gestiona la configuración AAA, Cisco Catalyst Center no tiene ningún conocimiento sobre si los dispositivos gestionados se configuran manualmente con el servidor AAA externo o si los dispositivos gestionados utilizan solo credenciales locales, de modo que asegúrese de que la contraseña se actualiza en el servidor AAA externo si se configura en los dispositivos gestionados afectados antes de continuar con estos pasos.

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).