

Firepower 4100/9300 FXOS Recuperación de contraseña de usuario local mediante acceso administrativo TACACS

Contenido

Problema

Se desconocía la contraseña de administrador local para FXOS en appliances Firepower 4100/9300, por lo que era necesario restablecerla para recuperar el acceso administrativo.

A todos los usuarios TACACS existentes solo se les asignó la función de solo lectura, lo que les impedía realizar tareas administrativas en el chasis FXOS.

Nota: A las cuentas de usuario autenticadas remotamente (LDAP, RADIUS, TACACS+, SSO) se les asigna el rol de solo lectura de forma predeterminada.

Entorno

- Cisco Firepower 4100/9300 con ASA/FTD
- Autenticación predeterminada de FXOS establecida en remota (Cisco ISE); autenticación local configurada como reserva.

Resolución

Crear un usuario TACACS administrativo

En Cisco ISE (o su servidor TACACS), cree un nuevo usuario TACACS (por ejemplo, fxosadmin) y asigne privilegios administrativos como se describe en la documentación de Cisco:

[Autenticación/autorización de chasis FXOS para administración remota con ISE mediante TACACS+.](#)

1. Crear los grupos de identidad y los usuarios
2. Cree el perfil de shell para cada rol de usuario (para el rol 'admin', utilice cisco-av-pair=shell:roles="admin")
3. Crear la política de autorización TACACS

Inicie sesión con el nuevo usuario administrador de TACACS

Utilice la cuenta recién creada fxosadmin para iniciar sesión en la GUI y CLI de FXOS. Esta

cuenta ahora tiene privilegios administrativos completos.

Restablecer la contraseña de administrador local

Acceda a la CLI de FXOS y ejecute estos comandos:

```
FP4100# scope security
FP4100 /security # show local-user
User Name      First Name      Last name
-----
admin
FP4100 /security # enter local-user admin
FP4100 /security/local-user # set password
Enter a password:
Confirm the password:
FP4100 /security/local-user* # commit-buffer
FP4100 /security/local-user #
```

Notas y consideraciones

- Cuando la autenticación remota (TACACS, RADIUS, LDAP, SSO) es el método predeterminado, no puede iniciar sesión en el Administrador de chasis de firewall con una cuenta de usuario local a menos que la autenticación remota no esté disponible.
- Las cuentas de usuario local y remota no se pueden utilizar indistintamente cuando la autenticación remota está activa.
- En este escenario, si el método de autenticación del puerto de la consola se establece en 'LOCAL', permite la verificación de las nuevas credenciales de administrador; de lo contrario, deberá desactivar la conectividad del servidor de autenticación remota para probar las credenciales de administrador.

Causa

- Se ha perdido o desconocido la contraseña de administrador local del chasis FXOS, lo que impide el acceso administrativo directo mediante la cuenta local.
- Todas las cuentas de usuario de TACACS existentes se configuraron con privilegios de solo lectura, lo que limitó la capacidad de realizar las tareas administrativas necesarias, como el reinicio del chasis, las actualizaciones y la copia de seguridad de FXOS, desde el acceso remoto.
- La situación creaba el riesgo de no poder administrar o recuperar el dispositivo si se necesitaban más cambios o resolución de problemas.
- Esto requería un restablecimiento de la contraseña de administrador para continuar con las actividades de mantenimiento planeadas.

Contenido relacionado

- [Gestión de usuarios de FXOS](#)
- [Procedimiento De Recuperación De Contraseña Para Dispositivos Firepower Serie 9300/4100](#)

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).