

Verificar el Comportamiento de Login con y sin AAA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Conclusión](#)

Introducción

Este documento explica el comportamiento del comando "login local" cuando la Autenticación, Autorización de Contabilización (AAA) está habilitada o inhabilitada en un router.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre los siguientes temas:

- Configuración AAA en routers de Cisco
- Radius/TACACS

Componentes Utilizados

La información de este documento se basa en las pruebas realizadas en varias versiones de Cisco IOS 12.2(22), 12.4T, 15.1M, 15.3M, etc. Sin embargo, este documento no se limita a versiones específicas de software y hardware.

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). If your network is live, make sure that you understand the potential impact of any command.

Configurar

A continuación se muestra la configuración mínima necesaria para verificar este comportamiento:

- Se puede alcanzar al menos un servidor de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) o de Sistema de control de acceso del controlador de acceso de terminal (TACACS+) desde el router sometido a la prueba.
- El router bajo prueba se reconoce como cliente del servidor AAA.
- Se configura la misma clave secreta previamente compartida en el router/switch de Cisco y en los servidores AAA remotos.
- Conjunto global de servidores RADIUS o subconjunto con nombre de servidores RADIUS o TACACS+ configurado en el router sometido a la prueba.
- Base de datos de usuario local configurada en el router sometido a la prueba.

Verificación

Cuando **'login local'** está configurado en **'line vty x'**, los usuarios podrán iniciar sesión usando el nombre de usuario y la contraseña locales configurados en el router. Pero cuando se configura **'aaa new-model'**, no hay configuración bajo **'line vty x'** porque ahora el método de inicio de sesión predeterminado es AAA.

Una vez que se guarda la configuración y se elimina AAA usando **'no aaa new-model'**, el método de inicio de sesión volverá a la autenticación de línea. La autenticación de línea se produce cuando el router solamente verifica la contraseña de línea y no la contraseña de nombre de usuario global configurada. Ahora no verá **'login local'** debajo de **'line vty x'**, que se configuró antes de habilitar AAA, sino que verá **'login'**.

Nota: No se recomienda desactivar AAA con "no aaa new-model".

Los siguientes pasos mostrarán este comportamiento en detalle:

Login local configured on router:

```
Router#show run | begin line vty
line vty 0 4
login local
```

Enable AAA on router:

```
Router(config)#aaa new-model

Router#show run | begin line vty
line vty 0 4
```

Save the configuration

```
Router#wr
Building configuration...
[OK]
```

Disable AAA

```
Router#conf t
Router(config)#no aaa new-model
Changing configuration back to no aaa new-model is not supported.
Continue?[confirm]
```

Check login method

```
Router#show run | begin line vty  
line vty 0 4  
  login
```

Conclusión

Al eliminar "AAA new-model", el método predeterminado será "login" bajo la línea y no "login local". Este comportamiento se observa en todas las versiones de Cisco IOS.

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).