

Verifique el comportamiento del login con y sin el AAA

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes usados](#)

[Configurar](#)

[Verificación](#)

[Conclusión](#)

Introducción

Este documento explica el comportamiento del comando del “login local” cuando la autenticación, las estadísticas de la autorización (AAA) se habilita o se inhabilita en un router.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de los temas siguientes:

- Configuración AAA en los routers Cisco
- Radius/TACACS

Componentes usados

La información en este documento se basa en la prueba realizada en la diversa versión deL Cisco IOS 12.2(22), 12.4T, el 15.1M, el 15.3M etc. Sin embargo, este documento no se restringe a las versiones de software y hardware específicas.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Lo que sigue es la configuración necesaria mínima para verificar este comportamiento:

- Por lo menos un servidor del Remote Authentication Dial-In User Service (RADIUS) o del Terminal Access Controller Access Control System (TACACS+) es accesible del router bajo prueba.
- Reconocen al router bajo prueba como cliente del servidor de AAA.
- La misma clave del Secreto previamente compartido se configura en el router Cisco/el Switch y los servidores de AAA remotos.
- Agrupación global de los servidores de RADIUS o subconjunto Nombrado de servidores RADIUS o TACACS+ configurados en el router bajo prueba.
- Base de datos de usuarios locales configurada en el router bajo prueba.

Verificación

Cuando el **“login local”** se configura bajo **“línea vty x”**, los usuarios podrán iniciar sesión usando el nombre de usuario local y la contraseña configurados en el router. Pero cuando el **“aaa de modelo nuevo”** se configura, no hay configuración bajo **“línea vty x”** porque ahora el método de inicio de sesión predeterminado es AAA.

Una vez que se guarda la configuración y el AAA se quita usando **“ningún AAA-nuevo modelo”**, el método de inicio de sesión volverá a la línea autenticación. La línea authentication es cuando el router apenas marca para saber si hay la contraseña de línea y no el username password global configurado. Ahora usted no verá el **“login local”** bajo **“línea vty x”** que fue configurada anteriormente habilitando el AAA, en lugar usted verá el **“login”**.

Nota: Inhabilitar el AAA con **“ningún aaa de modelo nuevo”** no se recomienda.

Los pasos siguientes mostrarán este comportamiento detalladamente:

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

Cuando usted quita el “AAA de modelo nuevo”, el método predeterminado será “login” bajo la línea y no “login local”. Este comportamiento se considera en todas las versiones deL Cisco IOS.