Verifica del comportamento di accesso con e senza AAA

Sommario

Introduzione

In questo documento viene illustrato il comportamento del comando "login local" quando l'autenticazione, l'accounting di autorizzazione (AAA) è abilitato o disabilitato su un router.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Configurazione AAA su router Cisco
- Radius/TACACS

Componenti usati

Le informazioni di questo documento si basano sui test eseguiti in diverse versioni di Cisco IOS: 12.2(22), 12.4T, 15.1M, 15.3M ecc. Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Di seguito è riportata la configurazione minima necessaria per verificare questo comportamento:

- Almeno un server RADIUS (Remote Authentication Dial-In User Service) o TACACS+ (Terminal Access Controller Access Control System) è raggiungibile dal router sottoposto a test.
- Il router sottoposto a test viene riconosciuto come client del server AAA.
- La stessa chiave segreta precondivisa è configurata sul router/switch Cisco e sui server AAA remoti.
- Pool globale di server RADIUS o sottoinsieme denominato di server RADIUS o TACACS+ configurati sul router sottoposto a test.
- Database utente locale configurato sul router sottoposto a test.

Verifica

quando si configura **'login local'** in **'line vty x'**, gli utenti saranno in grado di accedere usando il nome utente e la password locali configurati sul router. Tuttavia, quando si configura **'aaa new-model'**, non vi è alcuna configurazione nella **'line vty x'** perché il metodo di accesso predefinito è ora AAA.

Dopo aver salvato la configurazione e aver rimosso il server AAA con il comando "**no aaa-new model"**, il metodo di accesso tornerà all'autenticazione di linea. L'autenticazione di linea si ha quando il router cerca solo la password della linea e non la password del nome utente globale configurato. Ora non sarà possibile visualizzare '**login local'** in **'line vty x'** che era stato configurato prima di abilitare AAA, ma si vedrà **'login'.**

> **Nota**: si sconsiglia di disabilitare l'autenticazione AAA con "no aaa new-model".

Nei passaggi seguenti verrà illustrato in dettaglio questo comportamento:

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
```

Conclusioni

Quando si rimuove "AAA new-model", il metodo predefinito sarà "login" in linea e non "login local". Questo comportamento viene visualizzato su tutte le versioni di Cisco IOS.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).