

Esempio di configurazione di FreeRADIUS utilizzato per l'accesso amministrativo su Cisco IOS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione di uno switch per l'autenticazione e l'autorizzazione](#)

[Configurazione FreeRADIUS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione RADIUS sugli switch Cisco IOS® con un server RADIUS di terze parti (FreeRADIUS). In questo esempio viene illustrato come impostare un utente direttamente in modalità privilegio 15 dopo l'autenticazione.

Prerequisiti

Requisiti

Verificare che lo switch Cisco sia stato definito come client in FreeRADIUS con l'indirizzo IP e la stessa chiave segreta condivisa definiti in FreeRADIUS e nello switch.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- RaggioLibero
- Cisco IOS versione 12.2

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

Configurazione di uno switch per l'autenticazione e l'autorizzazione

1. Per creare un utente locale sullo switch con privilegi completi per l'accesso di fallback, immettere:

```
Switch(config)#username admin privilege 15 password 0 cisco123!
```

2. Per abilitare il server AAA, immettere:

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

3. Per fornire l'indirizzo IP del server RADIUS e la chiave, immettere:

```
switch# configure terminal
switch(config)#radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
switch(config)#radius-server key hello123
```

Nota: la chiave deve corrispondere al segreto condiviso configurato sul server RADIUS per lo switch.

4. Per verificare la disponibilità del server RADIUS, immettere il comando **test aaa**:

```
switch# test aaa server Radius 172.16.71.146 user1 Ur2Gd2BH
```

L'autenticazione di prova non riesce con un rifiuto da parte del server perché non è ancora configurato, ma confermerà che il server stesso è raggiungibile.

5. Per configurare le autenticazioni di accesso in modo che gli utenti locali possano eseguire il fallback se RADIUS non è raggiungibile, immettere:

```
switch(config)#aaa authentication login default group radius local
```

6. Per configurare l'autorizzazione per un livello di privilegio di 15, a condizione che un utente sia autenticato, immettere:

```
switch(config)#aaa authorization exec default group radius if-authenticated
```

Configurazione FreeRADIUS

Definire il client sul server FreeRADIUS

1. Per passare alla directory di configurazione, immettere:

```
# cd /etc/freeradius
```

2. Per modificare il file **clients.conf**, immettere:

```
# sudo nano clients.conf
```

3. Per aggiungere ciascun dispositivo (router/switch) identificato dal nome host e includere il segreto condiviso corretto, immettere:

```
client 192.168.1.1 {
  secret = secretkey
  nasstype = cisco
  shortname = switch
}
```

4. Per modificare il file degli utenti, immettere:

```
# sudo nano users
```

5. Aggiungere ogni utente autorizzato ad accedere al dispositivo. Nell'esempio viene mostrato come impostare un livello di privilegio di Cisco IOS pari a 15 per l'utente "cisco".

```
cisco Cleartext-Password := "password"
Service-Type = NAS-Prompt-User,
Cisco-AVPair = "shell:priv-lvl=15"
```

6. Per riavviare FreeRADIUS, immettere:

```
# sudo /etc/init.d/freeradius restart
```

7. Per modificare il gruppo di utenti PREDEFINITO nel file dell'utente in modo da assegnare a tutti gli utenti membri di cisco-rw il livello di privilegio 15, immettere:

```
DEFAULT Group == cisco-rw, Auth-Type = System
Service-Type = NAS-Prompt-User,
cisco-avpair := "shell:priv-lvl=15"
```

8. È possibile aggiungere altri utenti a diversi livelli di privilegi in base alle esigenze nel file degli utenti di FreeRADIUS. Ad esempio, a questo utente (life) viene assegnato il livello 3 (manutenzione del sistema):

```
sudo nano/etc/freeradius/users

life Cleartext-Password := "testing"
Service-Type = NAS-Prompt-User,
Cisco-AVPair = "shell:priv-lvl=3"

Restart the FreeRADIUS service:
sudo /etc/init.d/freeradius restart
```

Nota: la configurazione di questo documento si basa sull'esecuzione di FreeRADIUS su Ubuntu 12.04 LTE e 13.04.

Verifica

Per verificare la configurazione sullo switch, utilizzare questi comandi:

```
switch# show run | in radius      (Show the radius configuration)
switch# show run | in aaa        (Show the running AAA configuration)
switch# show startup-config Radius (Show the startup AAA configuration in
start-up configuration)
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- [RaggioLibero](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).