

FreeRADIUS voor administratieve toegang gebruikt op Cisco IOS-configuratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Een Switch voor verificatie en autorisatie configureren](#)

[Configuratie FreeRADIUS](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u RADIUS-verificatie op Cisco IOS[®]-switches kunt configureren met een RADIUS-server van derden (FreeRADIUS). Dit voorbeeld behandelt de plaatsing van een gebruiker direct in voorrecht 15 wijze op authenticatie.

Voorwaarden

Vereisten

Zorg ervoor dat u uw Cisco-switch hebt gedefinieerd als een client in FreeRADIUS met het IP-adres en dezelfde gedeelde geheime sleutel die op FreeRADIUS en de switch is gedefinieerd.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FreeRADIUS
- Cisco IOS-versie 12.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Een Switch voor verificatie en autorisatie configureren

1. Om een lokale gebruiker op de switch met volledige rechten voor reservetoegang te maken, voert u het volgende in:

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

2. Voer om AAA in te schakelen:

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

3. Als u zowel het IP-adres van de RADIUS-server als de sleutel wilt opgeven, voert u het volgende in:

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

Opmerking: de toets moet overeenkomen met het gedeelde geheim dat op de RADIUS-server voor de switch is geconfigureerd.

4. Voer de opdracht **aaa** van de **test** in om de beschikbaarheid van de RADIUS-server te testen:

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

De testverificatie mislukt met een afwijzing van de server omdat deze nog niet is geconfigureerd, maar het zal bevestigen dat de server zelf bereikbaar is.

5. Als u wilt dat lokale gebruikers kunnen terugvallen op aanmeldingsverificatie wanneer RADIUS onbereikbaar is, voert u het volgende in:

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

6. Als u de autorisatie voor een prioriteitsniveau van 15 wilt configureren, zolang een gebruiker is geverifieerd, voert u het volgende in:

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

Configuratie FreeRADIUS

De client op de FreeRADIUS-server definiëren

1. Om naar de configuratiemap te navigeren, voert u het volgende in:

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

2. Als u het bestand **clients.conf** wilt bewerken, voert u het volgende in:

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

3. Om elk apparaat (router/switch) dat wordt geïdentificeerd met hostname toe te voegen en het juiste gedeelde geheim op te nemen, voer je in:

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

4. Als u het gebruikersbestand wilt bewerken, voert u het volgende in:

```
# sudo nano users
```

5. Voeg elke gebruiker toe die toegang heeft tot het apparaat. Dit voorbeeld toont aan hoe u een Cisco IOS-prioriteitsniveau van 15 instelt voor de gebruiker "cisco".

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

6. Als u FreeRADIUS opnieuw wilt starten, voert u het volgende in:

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

7. Als u de STANDAARD gebruikersgroep in het bestand van de gebruiker wilt wijzigen om alle gebruikers die lid zijn van Cisco-rw een voorrangsniveau van 15 te geven, voert u het volgende in:

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

8. U kunt andere gebruikers toevoegen op verschillende niveaus van rechten zoals nodig in het FreeRADIUS gebruikersbestand. Deze gebruiker (life) krijgt bijvoorbeeld een niveau van 3 (systeemonderhoud):

```
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
```

Opmerking: de configuratie in dit document is gebaseerd op FreeRADIUS run op Ubuntu 12.04 LTS en 13.04.

Verifiëren

Gebruik de volgende opdrachten om de configuratie op de switch te controleren:

```
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)
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [FreeRADIUS](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.