

Exemple de configuration de FreeRADIUS utilisé pour l'accès administratif sur Cisco IOS

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Configurer un commutateur pour l'authentification et l'autorisation](#)

[Configuration de FreeRADIUS](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'authentification RADIUS sur les commutateurs Cisco IOS[®] avec un serveur RADIUS tiers (FreeRADIUS). Cet exemple couvre le placement d'un utilisateur directement en mode privilégié 15 lors de l'authentification.

Conditions préalables

Exigences

Assurez-vous que votre commutateur Cisco est défini en tant que client dans FreeRADIUS avec l'adresse IP et la même clé secrète partagée définie sur FreeRADIUS et le commutateur.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FreeRADIUS
- Cisco IOS version 12.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurer

Configurer un commutateur pour l'authentification et l'autorisation

1. Afin de créer un utilisateur local sur le commutateur avec des privilèges complets pour l'accès de secours, entrez :

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

2. Afin d'activer AAA, entrez :

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

3. Afin de fournir l'adresse IP du serveur RADIUS ainsi que la clé, entrez :

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

Remarque : la clé doit correspondre au secret partagé configuré sur le serveur RADIUS pour le commutateur.

4. Afin de tester la disponibilité du serveur RADIUS, entrez la commande **test aaa** :

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

Le test d'authentification échoue avec un refus du serveur car il n'est pas encore configuré, mais il confirme que le serveur lui-même est accessible.

5. Afin de configurer les authentifications de connexion pour qu'elles reviennent aux utilisateurs locaux si RADIUS est inaccessible, entrez :

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

6. Afin de configurer l'autorisation pour un niveau de privilège de 15, tant qu'un utilisateur est authentifié, entrez :

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

Configuration de FreeRADIUS

Définition du client sur le serveur FreeRADIUS

1. Pour accéder au répertoire de configuration, saisissez :

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

2. Afin de modifier le fichier **clients.conf**, entrez :

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

3. Afin d'ajouter chaque périphérique (routeur/commutateur) identifié par le nom d'hôte et d'inclure le secret partagé correct, entrez :

```
client 192.168.1.1 {
```

```
secret = secretkey
nastype = cisco
shortname = switch
}
```

4. Pour modifier le fichier des utilisateurs, saisissez :

```
# sudo nano users
```

5. Ajoutez chaque utilisateur autorisé à accéder au périphérique. Cet exemple montre comment définir un niveau de privilège Cisco IOS de 15 pour l'utilisateur « cisco ».

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

6. Afin de redémarrer FreeRADIUS, entrez :

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

7. Afin de modifier le groupe d'utilisateurs DEFAULT dans le fichier de l'utilisateur afin de donner à tous les utilisateurs qui sont membres de cisco-rw un niveau de privilège de 15, entrez :

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

8. Vous pouvez ajouter d'autres utilisateurs à différents niveaux de privilège, selon les besoins, dans le fichier utilisateurs FreeRADIUS. Par exemple, cet utilisateur (life) se voit attribuer un niveau de 3 (maintenance du système) :

```
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
```

Remarque : la configuration dans ce document est basée sur FreeRADIUS exécuté sur Ubuntu 12.04 LTE et 13.04.

Vérifier

Afin de vérifier la configuration sur le commutateur, utilisez ces commandes :

```
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)
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [FreeRADIUS](#)
- [Technical Support & Documentation - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.