

Sommaire

1. Installation des paquets pour disposer de freeradius sur le serveur	2
1.1. Installation des paquets	2
1.2. Edition du fichier clients.conf	3
1.3. Edition du fichier users	4
1.4. Edition du fichier radius.conf	4
1.5. Modification des droits	5
2. Installation des paquets sur la machine cliente	6
2.1. Installation des paquets	6
2.2. Test de la connexion côté client	6

Ce compte rendu permet l'installation et la configuration d'un serveur Radius ainsi que la configuration d'un client (serveur Linux)

Matériel nécessaire : 2 pc sous Linux : 1 serveur Radius + 1 client Linux

Les différentes installations seront faites sur 2 VMs Linux sous Debian 11

Avant de faire tout téléchargement il est nécessaire de mettre à jour nos machines :

```
Apt get update && upgrade
```

1. Installation des paquets pour disposer de freeradius sur le serveur

1.1. Installation des paquets

Pour pouvoir disposer d'un serveur radius nous avons besoin de télécharger les paquets suivants :

```
Apt install freeradius
```

Puis nous pouvons nous déplacer dans le dossier de freeradius :

```
Cd /etc/freeradius/3.0/
```

Ce répertoire contient tous les fichiers de configuration pour notre serveur radius. Les plus importants sont :

```
root@osboxes:/etc/freeradius/3.0# ls
certs          experimental.conf  mods-available    panic.gdb       radius.conf
sites-available trigger.conf
clients.conf   hints              mods-config       policy.d         radiusd.conf
sites-enabled  users
dictionary    huntgroups         mods-enabled      proxy.conf       README.rst
templates.conf
```

1^{er} fichier : /etc/freeradius/3.0/radiusd.conf :

Ce fichier contient les éléments principaux permettant la configuration de freeradius ainsi que les modules complémentaires

2^{ème} fichier : /etc/freeradius/3.0/clients.conf :

Ce fichier permet de gérer la configuration des clients qui se connectent au serveur (ici notre serveur Linux)

3^{ème} fichier : /etc/freeradius/3.0/users :

Ce fichier stocke toutes les informations concernant les utilisateurs (identifiant, mot de passe, informations personnelles...)

4^{ème} fichier : /etc/freeradius/3.0/radius.conf :

Ce fichier est un fichier non présent de base. C'est un fichier créé plus tard qui va permettre de configurer le port d'écoute du serveur ainsi que la gestion des logs

1.2. Edition du fichier clients.conf

Tout d'abord il va nous falloir configurer les clients distants qui vont se connecter à notre serveur (ici notre serveur Linux) :

```
Nano /etc/freeradius/3.0/clients.conf
```

Contenu du fichier (on ne touche pas à la configuration par défaut) :

```
#Client
client Linux-Server {
    ipaddr = 192.168.0.39/24
    proto = *
    secret = testing123
    require_message_authenticator = no
    nas_type = other

    limit {
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
    }
}
```

Surligné : Adresse IP du client distant

Surligné : Secret partagé entre les 2 machines (doit être identique des 2 côtés)

Surligné : Type d'équipement lié à cette adresse IP (ex : Cisco pour ce qui est switch, routeur)

1.3. Edition du fichier users

Maintenant nous allons devoir configurer un utilisateur avec son identifiant et son mot de passe :

```
Nano /etc/freeradius/3.0/users
```

Voici le contenu du fichier :

```
Sam      Cleartext-Password := "test"  
        Reply-Message := "Hello, %{User-Name}"
```

Surligné : Nom d'utilisateur lors de la connexion

Surligné : Mot de passe lié au nom d'utilisateur

Surligné : Message qui sera affiché dans le CLI lors du test de connexion

1.4. Edition du fichier radius.conf

Ce fichier est un fichier qui n'existe pas de base lors de l'installation de freeradius. Ce fichier permet de configurer le/les ports d'écoute du serveur :

```
Nano /etc/freeradius/3.0/radius.conf
```

Contenu du fichier :

```
listen {  
    type = auth  
    ipaddr = *  
    port = 1812  
}  
  
log {  
    destination = files  
    file = ${logdir}/radius.log  
    syslog_facility = daemon  
    stripped_named = no  
    auth = yes  
    auth_badpass = yes  
    auth_goodpass = yes  
}
```

Surligné : Permet de sélectionner sur quel type de connexion on ouvre le port (ici sur une authentification)

Surligné : Permet de définir sur quelle adresse IP on ouvre le port (ici sur toutes les IP)

Surligné : Permet de définir quel port sera ouvert sur le serveur

1.5. Modification des droits

Les nouveaux fichiers qui viennent d'être créés ne sont utilisables que par l'utilisateur « root » car c'est avec lui que nous avons apporté des modifications. Or le serveur radius utilise un utilisateur « freerad » pour tourner.

Vérification des droits sur les fichiers :

```
root@osboxes:/etc/freeradius/3.0# ls -al
total 156
drwxr-xr-x 9 freerad freerad 4096 12 août 11:26 .
drwxr-s--- 3 freerad freerad 4096 11 août 11:05 ..
drwxr-xr-x 2 freerad freerad 4096 11 août 11:05 certs
-rw-r----- 1 freerad freerad 2760 12 août 11:10 clients.conf
-rw-r----- 1 freerad freerad 1440  3 sept. 2021 dictionary
-rw-r----- 1 freerad freerad 2661  3 sept. 2021 experimental.conf
drwxr-xr-x 2 freerad freerad 4096 11 août 11:05 mods-available
drwxr-xr-x 9 freerad freerad 4096 11 août 11:05 mods-config
drwxr-xr-x 2 freerad freerad 4096 11 août 11:16 mods-enabled
-rw-r----- 1 freerad freerad 27990  3 sept. 2021 proxy.conf
-rw-r--r-- 1 root root 209 11 août 12:50 radius.conf
-rw-r----- 1 root root 30620  3 sept. 2021 radiusd.conf
... ..
```

Nous avons donc besoin de modifier les droits d'accès au fichier pour cet utilisateur :

```
chown freerad:freerad /etc/freeradius/3.0/radius.conf
chown freerad:freerad /etc/freeradius/3.0/radiusd.conf
chown freerad:freerad /etc/freeradius/3.0/mods-config/files/authorize
```

Une fois toutes ces modifications apportées dans les fichiers nous devons redémarrer le service afin qu'elles soient prises en compte :

```
service freeradius reload
```

2. Installation des paquets sur la machine cliente

2.1. Installation des paquets

Les paquets suivants ont besoin d'être installés sur la machine cliente afin de pouvoir effectuer des tests de connexion :

```
apt install libpam-radius-auth
apt install freeradius
```

2.2. Test de la connexion côté client

Maintenant nous pouvons effectuer un test de connexion depuis le client vers le serveur avec la commande radtest :

```
root@osboxes:/home/osboxes# radtest sam test 192.168.0.35 1812 testing123
Sent Access-Request Id 88 from 0.0.0.0:38934 to 192.168.0.35:1812 length 73
    User-Name = "sam"
    User-Password = "test"
    NAS-IP-Address = 192.168.0.39
    NAS-Port = 1812
    Message-Authenticator = 0x00
    Cleartext-Password = "test"
Received Access-Accept Id 88 from 192.168.0.35:1812 to 192.168.0.39:38934
length 32
    Reply-Message = "Hello, sam"
```

Nous avons bien un Access-Accept avec le « Hello » qui a été configuré précédemment dans le fichier users