

freeRADIUS

Serveur RADIUS libre, performant et modulaire
mais pas vraiment simple

Aurélien Geron, Wifirst, 7 janvier 2011

Plan

- Plusieurs protocoles :
RADIUS, EAP...
- Un serveur sous
GPLv2
- Un système de
configuration puissant
- Une multitude de
modules
- Comment écrire un
module ?



Source image: <http://crshare.com/abstract-backgrounds-vector-clipart/>

Le projet freeRADIUS

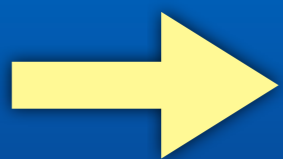
- FreeRADIUS (GPLv2) est un *fork* de Cistron (GPL) lui-même inspiré de Livingston (BSD)
- Commencé en 1999 par Alan DeKok et Miquel van Smoorenburg (auteur de Cistron)
- Disponible pour toutes les plateformes Un*x, MacOSX, et Windows (mais daté)
- Il devance maintenant la concurrence sur tous les plans (performance, fonctionnalités...)

La documentation

- Le point d'entrée de la documentation est :
<http://freeradius.org/doc/>
- Des infos utiles sont sur le Wiki, mais elles souvent datées ou incomplètes :
<http://wiki.freeradius.org/>
- Il y a beaucoup d'infos utiles dans les pages man :
<http://freeradius.org/radiusd/man/index.html>
- Lire aussi les commentaires des fichiers de config dans `/etc/freeradius` sous Debian (ou bien `/etc/raddb` sur la plupart des autres plateformes)

La documentation

- La liste de diffusion <http://freeradius.org/list/users.html> est réactive
- La documentation est un peu trop éparpillée, et parfois datée
- En outre, les informations que l'on peut trouver sur Internet (blogs, forums...) sont le plus souvent périmées et/ou fausses



Se méfier des infos trouvées sur les forums et blogs: vérifier la version

Installation

Sous Debian Squeeze

```
# la base
aptitude update
aptitude install freeradius

# puis ajouter les modules souhaités,
# par exemple:
aptitude install freeradius-mysql
```

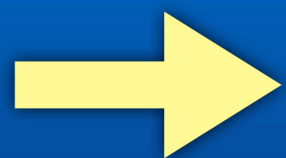
Les packages Debian

```
$ aptitude search freeradius
```

```
p   freeradius          - a high-performance and highly configurable RADIUS server
p   freeradius-common  - FreeRadius common files
p   freeradius-dbg     - ...; debug symbols
p   freeradius-dialupadmin - set of PHP scripts for administering a FreeRADIUS server
p   freeradius-iodbc   - iODBC module for FreeRADIUS server
p   freeradius-krb5    - kerberos module for FreeRADIUS server
p   freeradius-ldap    - LDAP module for FreeRADIUS server
p   freeradius-mysql   - MySQL module for FreeRADIUS server
p   freeradius-postgresql - PostgreSQL module for FreeRADIUS server
p   freeradius-utils   - FreeRadius client utilities
p   libfreeradius-dev  - FreeRADIUS shared library development files
p   libfreeradius2     - FreeRADIUS shared library
```

Et sous Debian Lenny ?

- Malheureusement, à cause d'un problème de licence, Debian ne fournissait pas freeRADIUS compilé avec OpenSSL
- Ce problème a été réglé dans la version 2.1.8 de freeRADIUS
- Mais la version de freeRADIUS incluse dans Debian Lenny est 2.0.4 (Squeeze est en 2.1.9)



Pour utiliser EAP/TLS, PEAP ou TTLS, dans Lenny : utiliser les backports

Backports pour Lenny

Voir: <http://www.backports.org/>

1. Add this line

```
deb http://www.backports.org/debian lenny-backports main contrib non-free
```

to your `/etc/apt/sources.list`.

2. Run `apt-get update`

3. All backports are deactivated by default (i.e. the packages are pinned to 1 by using `NotAutomatic: yes` in the Release files, just as in experimental). If you want to install something from backports run:

```
apt-get -t lenny-backports install "package"
```

Of course, you can use `aptitude` as well:

```
aptitude -t lenny-backports install "package"
```

You can also use pinning:

Then you have to set a higher priority for each backport, yes that means every backport, also for every dependency. For `mutt`, you have to add these lines:

```
Package: mutt
Pin: release a=lenny-backports
Pin-Priority: 999
```

to your `/etc/apt/preferences` (if you haven't use pinning before, the file has to be created).

After running `apt-get update` run `apt-get install mutt` as usual.

If you want `apt` to verify the downloaded backports you can import backports.org archive's key into `apt`:

```
apt-get install debian-backports-keyring
```

or

```
gpg --keyserver hkp://subkeys.pgp.net --recv-keys 16BA136C
gpg --export 16BA136C | apt-key add -
```

or

```
wget -O - http://backports.org/debian/archive.key | apt-key add -
```

If you want to get your packages from backports upgraded automatically the following entry in `/etc/apt/preferences` should be sufficient:

```
Package: *
Pin: release a=lenny-backports
Pin-Priority: 200
```

Compiler freeRADIUS

- Pour utiliser des modules expérimentaux ou pour les plateformes qui n'ont pas de package pour FreeRADIUS $\geq 2.1.8$
- Télécharger les sources et les compiler :
<http://freeradius.org/download.html>

```
$ tar zxvf freeradius-[version].tar.gz
$ ./configure # avec les options souhaitées
$ make
$ su - root
# make install
```

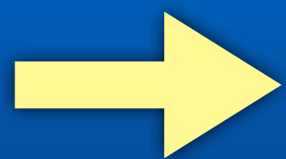
- Plus d'infos ici, notamment pour faire des packages propres pour Debian (ou pour d'autres distributions) :
<http://wiki.freeradius.org/Build>

Créer son propre package Debian

```
$ wget http://ftp.de.debian.org/debian/pool/main/f/freeradius/freeradius_2.1.9+dfsg-1.dsc
$ wget http://ftp.de.debian.org/debian/pool/main/f/freeradius/freeradius_2.1.9+dfsg.orig.tar.gz
$ wget http://ftp.de.debian.org/debian/pool/main/f/freeradius/freeradius_2.1.9+dfsg-1.diff.gz
$ tar xvzf freeradius_2.1.9+dfsg.orig.tar.gz
$ cd freeradius-server-2.1.9
$ zcat ../freeradius_2.1.9+dfsg-1.diff.gz | patch -p1
$ rm debian/patches/lt_dladvise.diff # => pour éviter une dépendance vers libtool 2.2
$ sed -i -e '/lt_dladvise.diff/d' debian/patches/series
$ dch -i # => préciser la version 2.1.9+dfsg-1~bpo50+1, des commentaires et coordonnées
$ dpkg-buildpackage -rfakeroot -uc -us -S
$ cd ..
$ sudo pbuilder --build freeradius_2.1.9+dfsg-1~bpo50+1.dsc
$ ls /var/cache/pbuilder/result/*freeradius*2.1.9*
```

freeRADIUS 2

- La version 1 manquait de clarté et de souplesse (fichiers de config pénibles)
- Les fichiers de config de la version 2 sont mieux organisés, et plus clairs
- Le module python (qui permet d'écrire des modules en python plutôt qu'en C) n'est plus expérimental et donc inclus par défaut dans les packages (avant il fallait tout recompiler pour l'inclure)



Utiliser de préférence freeRADIUS 2,
et si possible une version $\geq 2.1.8$

Les fichiers installés

```
$ dpkg -L freeradius | sort # puis raccourci à la main
/etc/freeradius
/etc/freeradius/eap.conf
/etc/freeradius/...
/etc/freeradius/modules
/etc/freeradius/modules/sql
/etc/freeradius/modules/...
/etc/freeradius/sites-available
/etc/freeradius/sites-available/default
/etc/freeradius/sites-available/inner-tunnel
/etc/freeradius/sites-available/...
/etc/freeradius/sites-enabled
/etc/freeradius/sites-enabled/default
/etc/freeradius/...
/etc/init.d/freeradius
/etc/logrotate.d/freeradius
/etc/pam.d/radiusd
/usr/lib/freeradius
/usr/lib/freeradius/rlm_sql-2.1.8.so
/usr/lib/freeradius/rlm_sql.so
/usr/lib/freeradius/...
/usr/sbin/checkrad
/usr/sbin/freeradius
/usr/sbin/raddebug
/usr/sbin/radmin
/usr/sbin/radwatch
/usr/share/doc/freeradius/...
/var/log/freeradius
```

ln -s

Ce répertoire ne contient que des liens symboliques vers les fichiers de `sites-available` que l'on souhaite utiliser (comme avec Apache)

FreeRADIUS est installé avec un module pam
(cf. http://fr.wikipedia.org/wiki/Pluggable_Authentication_Modules)

Ce binaire est le serveur freeRADIUS

Le script de démarrage/arrêt du serveur

Binaire des modules

Les fichiers installés

Dictionnaire RADIUS
(fichier personnalisable)

Point d'entrée de la
configuration du serveur
freeRADIUS

Les manuels : la liste est
intéressante à consulter :

```
dpkg -L freeradius-common
```

puis, par exemple:

```
man 5 acct_users
```

```
$ dpkg -L freeradius-common | sort # puis raccourci
/etc/freeradius
/etc/freeradius/dictionary
/etc/freeradius/radiusd.conf
/usr/share/doc/freeradius-common/...
/usr/share/freeradius
/usr/share/freeradius/dictionary
/usr/share/freeradius/dictionary.3com
/usr/share/freeradius/dictionary.3gpp
/usr/share/freeradius/dictionary.3gpp2
/usr/share/freeradius/dictionary.acme
/usr/share/freeradius/dictionary.airespace
/usr/share/freeradius/dictionary.alcatel
/usr/share/freeradius/dictionary...
/usr/share/man/man1
/usr/share/man/man1/radclient.1.gz
/usr/share/man/man1/radeapclient.1.gz
/usr/share/man/man1/...
/usr/share/man/man5
/usr/share/man/man5/acct_users.5.gz
/usr/share/man/man5/clients.conf.5.gz
/usr/share/man/man5/...
/usr/share/man/man8
/usr/share/man/man8/freeradius.8.gz
/usr/share/man/man8/raddebug.8.gz
/usr/share/man/man8/...
```

\$INCLUDE

\$INCLUDE

Fichiers à ne pas
modifier

Démarrer / arrêter

```
$ /etc/init.d/freeradius
```

```
Usage: /etc/init.d/freeradius start|stop|restart|force-reload
```

Débugger

```
$ /etc/init.d/freeradius stop
```

```
Stopping FreeRADIUS daemon: freeradius.
```

```
$ freeradius -X
```

```
FreeRADIUS Version 2.1.8, for host x86_64-pc-linux-gnu, built on Jan  3 2010 at 14:14:04
```

```
Copyright (C) 1999-2009 The FreeRADIUS server project and contributors.
```

```
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A  
PARTICULAR PURPOSE.
```

```
You may redistribute copies of FreeRADIUS under the terms of the  
GNU General Public License v2.
```

```
Starting - reading configuration files ...
```

```
including configuration file /etc/freeradius/radiusd.conf
```

```
including configuration file /etc/freeradius/proxy.conf
```

```
...
```

```
listen {
```

```
    type = "auth"
```

```
    ipaddr = 10.1.2.3
```

```
    port = 0
```

```
}
```

```
listen {
```

```
    type = "acct"
```

```
    ipaddr = 10.1.2.3
```

```
    port = 0
```

```
}
```

```
Listening on authentication address 10.1.2.3 port 1812
```

```
Listening on accounting address 10.1.2.3 port 1813
```

```
Listening on proxy address 10.1.2.3 port 1814
```

```
Ready to process requests.
```




Questions ?