Proftpd

Eric BERTHOMIER

1 Installation

- Installation du pakage par `apt-get install proftpd`.
- Modification du fichier `/etc/inetd.conf` en changeant ou ajoutant la ligne concernant le ftp.
  `ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/proftpd`.
- Relancer `inetd` : `killall -HUP inetd`.
  Tester avec ftp localhost.

2 Modification de la configuration

Le fichier de configuration est `/etc/proftpd.conf`. La documentation se trouve dans /usr/doc/propftpd. Pour qu'une modification soit prise en compte, il faut stopper et redémarrer le démon :

- `start-stop-daemon -K -exec /usr/sbin/proftpd`
- `start-stop-daemon -S -exec /usr/sbin/proftpd`

ou sur une distribution de type RedHat :

- `/etc/rc.d/init.d/<nom du démon> start`
- `/etc/rc.d/init.d/<nom du démon> stop`
- `/etc/rc.d/init.d/<nom du démon> restart`

De manière générale, on peut forcer un démon à relire son fichier de configuration en tapant la commande :

```
kill -HUP <no_process_daemon>
```

3 Ajout et modifications

3.1 Protections

`DefaultRoot ~` : l'utilisateur est confiné au répertoire de base qui lui est donné à la connexion.
`Umask 0137` : permet d'avoir les droits `-rw-r---`. Le `w` pour l'utilisateur est obligatoire pour pouvoir réécrire ou supprimer un fichier.

3.2 Message de bienvenue

```
<Global>
   DisplayLogin welcome.msg
</Global>
```

Comme `DefaultRoot ~`, le message de bienvenue doit se trouver sur le répertoire de connexion de l'utilisateur FTP.

4 Configuration de Linux

4.1 Utilisateurs et groupes

Attention par défaut `proftpd` utilise le groupe `nogroup` pour fonctionner. Pensez à le créer s'il n'existe pas déjà.

1. Création d'un utilisateur de base `majeis` qui pourra modifier le contenu du répertoire. Répertoire de base `/home/majeis`. `adduser majeis -home ...`
2. Création d'un utilisateur invité `invite` qui pourra lire le répertoire. Répertoire de base `/home/majeis`. `adduser invite -home /home/majeis`
3. Création d'un compte ftp wwwftp : `addgrp wwwftp`.
4. Affiliation des utilisateurs au groupe wwwftp : édition du fichier `/etc/group` ajout à la fin de la ligne `wwwftp` majeis,invite

Extrait du fichier `/etc/group`

```
invite:*:1008:
majeis:*:1009:
nogroup:x:1010:
ftpwww:x:1011:majeis,invite
```

4.2 Ajouts de fichiers, problèmes de groupes

Afin que les fichiers appartiennent au groupe `wwwftp` et non au groupe `majeis`, il est nécessaire que `majeis` appartiennent d'abord au groupe wwwftp. Le but est d'obtenir lors de l'exécution de la commande `id` : `uid=1007(majeis)` **gid=1011(wwwftp)** `groupes=1011(wwwftp)`. Pour celà on modifie le fichier `/etc/passwd` de manière à ce que le gid de `majeis` soit `wwwftp` (1011).

Extrait du fichier `/etc/passwd`

```
invite:x:1008:1008::/home/majeis:/bin/bash
majeis:x:1007:1011::/home/majeis:/bin/bash
```

4.3 Prise en compte des modifications dans /etc/group et /etc/passwd

En root (`su` insuffisant), reconstruire le fichier `/etc/shadow` grâce à la commande `pwconv`.

4.4 Répertoire

Vérifiez que le répertoire `/home/majeis` est les droits drwxr—–. Le droit d'exécution est obligatoire au moins pour le propriétaire.

5 Exemple de répertoire configuré

```
total 432
drwxr-x---    2 majeis   ftpwww      4096 sep 28 10:51 .
drwxr-x--x   10 majeis   ftpwww      4096 sep 27 16:54 ..
-rw-r-----    1 majeis   ftpwww    428032 sep 28 10:51 WS_FTP95.exe
```

6 Erreurs

`DisplayConnect`, je n'ai pas réussi vraiment à le faire fonctionner, entrainaît le refus de toute connexion.

7 Accès direct via navigateur

L'adresse du site sera composé de la façon suivante :

ftp ://<user> :<password>@<ip>

où
- `<user>` représent le nom de l'utilisateur.
- `<password>` le mot de passe qui lui est associé.
- `<ip>` l'adresse ip de la machine ou le nom de domaine qui lui est associé.

8 Exemple de fichier proftpd.conf

```
# This is a basic ProFTPD configuration file (rename it to
# 'proftpd.conf' for actual use.  It establishes a single server
# and a single anonymous login.  It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.

ServerName "Serveur FTP EIS"
ServerType standalone
DefaultServer on

DefaultRoot ~

# Port 21 is the standard FTP port.
Port 21
# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
# Droits de
Umask 0137

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances 30

# Set the user and group that the server normally runs at.
User nobody
Group nogroup

# Don't let people pass % character to the server
DenyFilter %

<Global>
  DisplayLogin welcome.msg
</Global>

# Limitation des logins
<Limit LOGIN>
  order deny,allow
  DenyUser all
  AllowUser webmaster
  AllowUser majeis
  AllowUser invite
</Limit>

# Normally, we want files to be overwriteable.
<Directory /*>
  AllowOverwrite on
</Directory>
```