Configuration de pure-ftpd

1. Présentation de pure-ftpd

Pure-ftp est un serveur ftp performant, sûr (c'est qu'ils disent dans la doc.) et assez simple à configurer, mais tout est relatif.

2. Installation

Avec debian en tant qu'utilisateur root :

```
# aptitude update; aptitude install pure-ftpd
```

Répondre aux questions :
 ... lancer pure-ftpd à partir de inetd ou serveur autonome : <serveur autonome>
 ... pure-ftpwho avec les droits superutilisateur ? : <Non>

Si ces questions ne vous ont pas été posées ou si vous constatez que pure-ftpd n'est pas lancé au démarrage, assurez-vous que la ligne suivante est bien présente et non commentée dans le fichier */etc/default/pure-ftpd-common* :
STANDALONE_OR_INETD=standalone

Le serveur ftp se présente sous la forme d'un binaire qui n'a pas besoin de fichiers de configuration! Tout est passé en paramètres de la ligne de commande lorsqu'on lance le serveur :

```
/etc/pure-ftpd# /etc/init.d/pure-ftpd start
Starting ftp server: Running: /usr/sbin/pure-ftpd -l puredb:/etc/pure-ftpd/pureftpd.pdb -u 120 -j
-O clf:/var/log/pure-ftpd/transfer.log -i -p 49152:65534 -B
```

Du coup, sous Debian, ils ont fait un wrapper, c'est à dire un logiciel qui fabrique automatiquement les paramètres de la ligne de commande. Et biensûr ce wrapper a besoin de fichiers de configuration !!!

Ces fichiers de configuration sont stockés dans /etc/pure-ftpd/conf/ et /etc/pure-ftpd/auth/
Le wrapper utilise un fichier de configuration du répertoire /etc/pure-ftpd/conf/ pour chaque option sur la ligne de commande de pure-ftpd. Le répertoire /etc/pure-ftpd/auth/ ne contient que des liens logiques qui dressent la liste des systèmes d'authentification que doit utiliser pure-ftpd. Pour plus de détails :

```
# man pure-ftpd
# man pure-ftpd-wrapper
```

Et l'excellente documentation en ligne sur le site http://www.pureftpd.org

3. Principe de fonctionnement

a. Les options de lancement du daemon

Elles sont nombreuses et décrites très clairement dans la documentation.

Voici quelques options que l'on peut utiliser, d'autres sont décrites plus loin :

```
# /usr/sbin/pure-ftpd -b -B -c 5 -C 3 -E -H -K -I 30 -l puredb:/etc/pure-ftpd/pureftpd.pdb
```

Dans cet exemple, nous avons:

- Le serveur est lancé en mode daemon et assure une compatibilité avec certains clients (-b -B)
- Le serveur peut avoir jusqu'à 5 connections simultanées dont 3 seulement de la même IP (-c 5 -C 3)
- Les utilisateurs anonymes sont refusé (-E)
- Les logs contiennent seulement les IP, donc pas de résolution de noms (-H)
- Permet de télécharger et de reprendre des téléchargements en cours, mais interdit de les

supprimer. Des répertoires peuvent être supprimés, mais seulement s'ils sont vides (-K).

- Le timeout est porté de 15 à 30 minutes (-I 30)
- Le serveur utilisera uniquement les utilisateurs virtuels pour l'authentification (-l puredb:/etc/pure-ftpd/pureftpd.pdb).

b. Les utilisateurs virtuels

L'authentification peut utiliser un intéressant mécanisme s'appuyant sur des utilisateurs virtuels. On créé de tels utilisateurs qui ne sont pas reconnus par unix mais seulement par le serveur pureftpd. Tous ces utilisateurs virtuels devront être mappés sur un utilisateur unix. Ils pourront, par exemple, être tous mappés sur le même uid et gid unix. Les paramètres de ces utilisateurs virtuels sont stockés dans 2 fichiers /etc/pure-ftpd/pureftpd.passwd (fichier ASCII) et /etc/pure-ftpd/pureftpd.pdb (fichier binaire).

Méthode standard pour créer un utilisateur virtuel:

Exemple de création manuelle de l'utilisateur virtuel « **user** » avec /home/user comme homedir :

```
# pure-pw useradd user -u 120 -g 120 -d /home/user -m
```

Le compte est ajouté au fichier /etc/pure-ftpd/pureftpd.passwd qui ressemble beaucoup à /etc/passwd mais avec plus d'options.
Attention, ce fichier n'est jamais directement utilisé par le daemon pureftpd.

l'option -m permet que cet ajout soit pris en compte tout de suite et soit aussi stocké dans la base /etc/pure-ftpd/pureftp.pdb (fichier binaire) qui est directement utilisé par le daemon pure-ftpd.

le -d pour un homedir chrooté : l'utilisateur est bloqué dans son répertoire (-D pour un homedir non chrooté).

Pour reconstruire la base /etc/pure-ftpd/pureftpd.pdb à partir de /etc/pure-ftpd/pureftpd.passwd :

Si on modifie à la main le fichier pureftpd.passwd ou que l'on utilise pure-pw sans l'option -m, il est nécessaire de mettre à jour pureftpd.pdb pour que les modifications soient prises en compte par le daemon pure-ftpd (sans même avoir besoin de le redémarrer) :

```
# pure-pw mkdb
```

Pour changer le mot de passe de l'utilisateur virtuel « user » :

```
# pure-pw passwd user -m
```

Pour voir les paramètres de l'utilisateur virtuel « user » :

```
# pure-pw show user
```

```
/etc/pure-ftpd# pure-pw show user

Login              : user
Password           : $1$za$SFqCCMVIJhGk0RrFTFSAi.
UID                : 120 (ftpuser)
GID                : 120 (ftpgroup)
Directory          : /home/user/./
Full name          : Exemple de user
Download bandwidth : 0 Kb (unlimited)
Upload   bandwidth : 0 Kb (unlimited)
Max files          : 0 (unlimited)
Max size           : 0 Mb (unlimited)
Ratio              : 0:0 (unlimited:unlimited)
Allowed local  IPs :
```

```
Denied  local  IPs :
Allowed client IPs :
Denied  client IPs :
Time restrictions  : 0000-0000 (unlimited)
Max sim sessions   : 0 (unlimited)
```

On peut voir qu'il y a d'intéressantes options de configurations des utilisateurs et notamment la gestion de quotas et de la bande passante !
Pour les nombreuses autres possibilités (usermod, userdel,...) voir le man:

```
# man pure-pw
```

c. L'accès anonymous ou ftp

Pour l'accès anonymous il suffit de créer un utilisateur unix nommé 'ftp' avec son home directory qui pointe sur la zone publique.

Dans la zone publique, pas besoin de répertoires ou commandes spéciaux (bin, etc, ls, ...) contrairement à d'autres serveurs ftp.

4. Détail de configuration – Un exemple particulier

a. Options de lancement du daemon pure-ftpd

Voilà un exemple d'options utilisés pour le lancement du daemon lors d'un /etc/init.d/pure-ftpd restart :

```
/usr/sbin/pure-ftpd -l puredb:/etc/pure-ftpd/pureftpd.pdb -u 120 -j -O clf:/var/log/pure-ftpd/transfer.log -i -p 49152:65534 -B
```

b. Seulement des utilisateurs virtuels

Cette configuration accepte seulement des utilisateurs virtuels qui sont mappés sur l'utilisateur unix ftpuser (uid=120, gid=120).

```
# grep ftpuser /etc/passwd
ftpuser:x:120:120::/dev/null:/etc
```

```
# grep ftpgroup /etc/group
ftpgroup:x:120:
```

Tous les utilisateurs virtuels sont chrootés sur leur home directory (= ils ne peuvent pas remonter l'arborescence des répertoires).

c. L'accès anonymous autorisé mais sans upload

L'accès anonymous est autorisé sur le serveur avec interdiction d'uploader des fichiers. On a donc un utilisateur unix nommé ftp.

```
# grep ftp: /etc/passwd
ftp:x:121:121::/ftp/PUBLIC:/bin/false
```

L'ajout d'un utilisateur virtuel « spécial » peut permettre d'uploader dans la zone publique.

d. Les fichiers de configuration /etc/pure-ftpd/conf/

Voici un exemple de fichiers de configurations qui permettent de lancer le daemon pure-ftpd avec les options vu en 4.a):

```
/etc/pure-ftpd/conf# ls -1
AltLog
AnonymousCantUpload
CreateHomeDir
FortunesFile
MaxClientsNumber
MinUID
NoAnonymous
NoChmod
```

```
PAMAuthentication
PassivePortRange
PureDB
Umask
UnixAuthentication
VerboseLog
```

Et voilà ce que contiennent ces fichiers (le contenu se trouve après « => », soit toujours une ligne par fichier)

```
AltLog              => clf:/var/log/pure-ftpd/transfer.log
AnonymousCantUpload => yes
CreateHomeDir       => yes
MinUID              => 120
NoAnonymous         => no
NoChmod             => yes
PAMAuthentication   => no
UnixAuthentication  => no
PassivePortRange    => 49152 65534
PureDB              => /etc/pure-ftpd/pureftpd.pdb
Umask               => 133 022
VerboseLog          => no
```

Par rapport à l'installation debian standard :

- la PAMAuthentication et l'UnixAuthentication sont desactivés. Un utilisateur standard unix ne peut pas utiliser le ftp (PAMAuthentication => no et UnixAuthentication => no),
- les anonymous sont autorisés (NoAnonymous => no),
- l'upload pour les anonymous est interdit (AnonymousCantUpload => yes),
- l'uid minimum est fixé à 1000 par defaut pour autoriser 'ftpuser' (uid 120) pour les utilisateurs virtuels,
- la création automatique du homedir d'un nouvel utilisateur est permise. (CreateHomeDir => yes). Pas besoin donc de faire le « mkdir ... »,
- une plage de ports pour le mode passif est spécifiée (49152 à 65534, ces ports sont ouverts sur le routeur),
- le chmod est interdit (NoChmod => yes),
- les droits des fichiers et répertoires sont forcés (Umask => 133 022),
- le niveau de log est redéfini (VerboseLog),
- le format et l'emplacement des logs de transferts avec GET et PUT est redéfini (AltLog).

Remarque :

Mettre à « yes » le contenu du fichier VerboseLog permet de logguer tout ce qui se passe sur le serveur dans /var/log/syslog et /var/log/messages. Pour éviter tous ces logs on peut soit mettre VerboseLog à « no », soit effacer le fichier. Les transferts upload/download sont loggués dans /var/log/pure-ftpd/transfer.log (cf fichier conf/AltLog)

Autres exemples de fichiers de configuration :

-> Pour porter le nombre de clients simultanés de 50 (valeur par défaut) à 100 :

```
# echo "100" > /etc/pure-ftpd/conf/MaxClientsNumber
```

et on relance pure-ftpd :

```
# /etc/init.d/pure-ftpd restart
Restarting ftp server: Running: /usr/sbin/pure-ftpd -l puredb:/etc/pure-ftpd/pureftpd.pdb -u 120 -j
-O clf:/var/log/pure-ftpd/transfer.log -i -p 49152:65534 -c 100 -B
```

-> Pour afficher une maxime littéraire lorsqu'on se loggue au serveur ftp :

Tout d'abord, il faut installer le paquet debian qui contient ces maximes littéraires (si ce n'est pas déjà fait) :

```
# aptitude install fortunes-fr
```

La liste des maximes à installer est proposée, on peut choisir de les installer toutes.

Ajouter le fichier de configuration qui va bien, avec en paramètre le chemin qui conduit au fichier texte des maximes littéraires :

```
# echo "/usr/share/games/fortunes/fr/litterature_francaise" > /etc/pure-ftpd/conf/FortunesFile
```

et on relance pure-ftpd :

```
# /etc/init.d/pure-ftpd restart
Restarting ftp server: Running: /usr/sbin/pure-ftpd -l puredb:/etc/pure-ftpd/pureftpd.pdb -u 120 -j
-F /usr/share/games/fortunes/fr/litterature_francaise -O clf:/var/log/pure-ftpd/transfer.log -i -p
49152:65534 -c 100 -B
```

e. Les fichiers de configuration pour l'authentification /etc/pure-ftpd/auth/

Le répertoire /etc/pure-ftpd/auth contient des liens symboliques sur les systèmes d'authentification. Au cours de l'installation de pure-ftpd 2 systèmes d'authentification sont pré-configurés :

```
/etc/pure-ftpd/auth# ls -l
lrwxrwxrwx  1 root root 26 2005-08-12 09:35 65unix -> ../conf/UnixAuthentication
lrwxrwxrwx  1 root root 25 2005-08-12 09:31 70pam -> ../conf/PAMAuthentication
```

Pour autoriser, le mécanisme d'authentification des utilisateurs virtuels, il faut ajouter un lien supplémentaire :

```
/etc/pure-ftpd/auth# ln -s ../conf/PureDB 75puredb
```

La PAMAuthentication et l'UnixAuthentication peuvent être desactivés (cf le contenu des fichiers /etc/pure-ftpd/conf/PAMAuthentication et /etc/pure-ftpd/conf/UnixAuthentication). Il aurait été possible de supprimer les liens dans /etc/pure-ftpd/auth pour desactiver ces modes d'authentification.

Actuellement, on a donc :

```
/etc/pure-ftpd/auth# ls -l
lrwxrwxrwx  1 root root 26 2005-08-12 09:35 65unix -> ../conf/UnixAuthentication
lrwxrwxrwx  1 root root 25 2005-08-12 09:31 70pam -> ../conf/PAMAuthentication
lrwxrwxrwx  1 root root 14 2005-08-09 10:07 75puredb -> ../conf/PureDB
```

Remarques :

- l'ordre alphabétique des liens détermine l'ordre utilisé par pure-ftpd pour la méthode d'authentification des utilisateurs du ftp (l'ordre des -l sur la ligne de commande)
- Si l'utilisateur est connu d'une méthode d'authentification mais que celle-ci échoue, la connection est refusée sans tester les éventuelles méthodes suivantes. Dans notre cas, nous utilisons seulement la méthode PureDB.

Astuces :

On peut créer plusieurs utilisateurs virtuels qui pointent sur le même répertoire:

Cette « astuce » permet de donner un accès complet à un compte utilisateur sans fournir le mot de passe de l'utilisateur original.

Une autre astuce est de procéder comme précédemment mais de mettre l'uid 121 à la place de 120 pour le nouvel utilisateur virtuel. Celui-ci n'a alors qu'un accès en lecture au compte.

—

Guy Roussin, le 2 Mai 2006.