

Serveur FTP

Julien Danjou
jdanjou@linuxenrezo.org

1 Installation du serveur

Vous devez installer un serveur, tel BeroFTPD ou wu-ftp. Wu-ftp connaît certains problèmes de sécurité et il est donc préférable d'utiliser BeroFTPD.

Vous pouvez vous les procurer sur leurs sites respectifs (cherchez sur <http://www.linuxapps.com>).

Installez les comme expliqué dans l'archive, ou à partir d'un package spécifique à votre distribution (rpm pour Redhat/Mandrake, deb pour Debian...).

Pour ces explications, j'ai utilisé **BeroFTPD**.

2 Installation des répertoires

Il se peut que les différents fichiers et répertoires indiqués ci dessous aient été créés lors de l'installation du serveur. Si c'est le cas, vérifiez seulement qu'ils ont correctement été créés, avec les bonnes permissions.

Tout d'abord, ajoutez un nouvel utilisateur ftp dans `/etc/passwd`.

Ajoutez aussi un groupe ftp dans `/etc/group`. Son répertoire d'accueil doit être `/home/ftp`.

Voilà un exemple:`/etc/passwd`

```
ftp*:14:50:FTP User:/home/ftp:  
/etc/group  
ftp::50:
```

Créez ensuite le répertoire `/home/ftp` et attribuez lui le mode 555, le propriétaire devant en être root.

Créez le répertoire `/home/ftp/bin` appartenant à root. avec les droits d'accès 111. Copiez dans ce répertoire le programme `ls` qui devra appartenir à root et

avoir les droits d'accès 111. Si vous copiez ultérieurement des programmes dans ce répertoire, il devront aussi appartenir à root avec les droits d'accès 111.

Créez le répertoire `/home/ftp/etc` appartenant à root, avec les droits 444. Vous devriez y placer un fichier `passwd` de ce type:

```
root:*:0:0:::
bin:*:1:1:::
operator:*:11:0:::
ftp:*:14:50:::
nobody:*:99:99:::
```

Et un fichier `group`:

```
root::0:
bin::1:
daemon::2:
sys::3:
adm::4:
ftp::50:
```

Vous pouvez les modifier selon l'UID et le GID choisis dans le fichier `/etc/passwd`.

Créez le répertoire `/home/ftp/pub`. Il doit appartenir à root et au groupe ftp. Tout ce qui sera dans ce répertoire sera accessible publiquement.

Tout ce qui s'y trouve devra posséder les droits 555. Si vous désirez que des utilisateurs anonymes puissent déposer des fichiers, créez un répertoire `/home/ftp/incoming`, puis faites un:

```
chmod +t/home/ftp/incoming
```

Cela empêchera quiconque d'écraser un fichier existant !

Il est bon, si possible, que créer votre répertoire ftp dans une partition différente de votre partition principale: en effet, si une personne (plutôt mal intentionnée...) se met à envoyer dans le répertoire `incoming` des dizaines d'énormes fichiers, votre partition principale risque d'être pleine, et votre machine complètement paralysée !!!

Si vous montez des partitions dans votre répertoire ftp, pensez à les monter en lecture seule !

3 Le fichier de configuration

Le fichier de configuration du serveur FTP est `/etc/ftpaccess`. Il est composé de différents paramètres, chacun utilisant une ligne...

Voici ces principaux paramètres :

deny addrglob message_file

Refuse l'accès à toutes les machines ayant pour adresse `addrglob` et affiche le message `message_file`. Vous pouvez mettre `!nameserved` comme valeur pour `addrglob` afin de refuser les connexions venant des hôtes sans enregistrement de nom inverse dans leur serveur de nom; ou le chemin d'un fichier commençant par `par`, contenant les hôtes refusés sous la forme `adresse:netmask`.

guestgroup groupname [groupname ...]

guestuser username [username ...]

realgroup groupname [groupname ...]

realuser username username ...]

Pour `guestgroup`, si n'importe quel utilisateur réel appartient à un des groupes spécifiés, sa session sera comme celle d'un utilisateur anonyme.

`groupname` doit être un groupe valide de `/etc/group`. Le répertoire d'accueil de l'utilisateur doit être configuré dans le fichier `/etc/passwd`.

Le premier champ sera le répertoire racine, le deuxième le répertoire d'accueil. Les 2 paramètres devront être séparés par `./`.

Exemple dans `/etc/passwd`:

```
guest1:passwd:100:92:Guest Account:/ftp/./incoming:/etc/ftponly
```

Quand `guest1` sera loggé, son répertoire racine sera `/ftp` et son répertoire d'accueil sera `/incoming`. Il ne pourra accéder qu'au répertoire et fichiers se trouvant sous `/ftp`, qui pour lui s'apparentera à `/`.

Le nom du groupe peut être un ID numérique, mais vous devez alors placer un `%` devant le nombre. Mettre un `*` signifie tout les groupes.

`realuser` et `realgroup` ont la même syntaxe, mais à l'effet inverse. Ils autorisent un utilisateur à avoir un accès normal, alors qu'il devrait avoir un accès de type `guest`.

Par exemple:

```
guestuser *  
realgroup admin
```

a pour cause de traiter tous les utilisateurs non anonymes en tant qu'utilisateurs anonymes, sauf les utilisateurs appartenant au groupe admin, qui eux seront traités normalement.

guestserver [hostname]

Spécifie les clients qui sont autorisés à se connecter en tant qu'utilisateur anonyme. Si aucune valeur n'est spécifié, aucun accès anonyme n'est autoris.

noretrieve [absolute|relative|-] filename filename

Toujours refuser le téléchargement de ces fichiers. Si le fichier est un chemin absolu (ex: il commence avec un /), tous ces fichiers seront marqués comme impossible à récupérer, autrement tous les fichiers correspondant à filename verront leur transfert refusé.

Exemple:`noretrieve /etc/passwd core`
spécifie que le transfert de `/etc/passwd` ou d'un fichier s'appelant `core` sera refusé. En revanche, un fichier s'appelant `passwd`, mais se trouvant ailleurs que dans `/etc/` verra son transfert autorisé.

Il est possible de spécifier un répertoire. Dans ce cas, tout les fichiers qu'il contient ne seront pas téléchargeables.

Le premier paramètre est optionnel, et sert à sélectionner si les noms de fichiers ou de répertoires doivent être interprétés comme absolus ou relatifs. La valeur par défaut est d'interpréter les noms commençant par un / comme absolus.

```
allow-retrieve [absolute|relative|-] filename  
filename
```

Autorise le transfert de fichiers qui autrement serait refusé par `noretrieve`.

loginfails number

Après `number` d'erreur de login, enregistrer un message de `repeated login failure` et terminer la connexion FTP. La valeur par défaut est 5.

greeting full|brief|terse

Contrôle combien d'informations sont données avant l'invite de login. Full est par défaut et montre le nom d'hôte et la version du daemon. Brief montre le nom d'hôte seulement, et terse dit seulement FTP server ready. Même si full est par défaut, brief est recommandé.

banner path

Ressemble à la commande message, mais apparait AVANT l'invite de login/password. Le chemin est relatif à la racine réelle et non à celle du serveur FTP anonyme.

hostname some.host.name

Définit le nom d'hôte du serveur FTP. Il est envoyé lors de la connection avec l'option greeting full.

email name

Définit l'adresse e-mail du responsable du serveur.

message path {when {class}}

Définit le fichier que ftpd affichera à l'utilisateur au moment du login ou de changement de répertoire. Le paramètre when peut être LOGIN ou CWD=dir. Si when est CWD=dir, dir spécifie le nouveau répertoire par défaut qui fera afficher le message. On peut utiliser des magic cookies dans les fichiers. Le serveur FTP remplacera ces cookies par leur valeur, tel que:

%T Heure local (forme Thu Nov 15 17:12:42 1990)

%C Répertoire courant

%E L'adresse e-mail de l'administrateur spécifié dans /etc/ftppass

%R Nom d'hôte du client

%L Nom d'hôte du serveur

%U Nom d'utilisateur donné

%M Nombre d'utilisateur maximum dans cette classe

%N Nombre d'utilisateur en ce moment dans cette classe

%q Nombres d'inodes alloués.

Si vous utilisez la limitation de téléchargement, vous pouvez aussi utiliser:

%xu Bits envoyés

%xd Bits reçus

%xR Envoie/réception ratio (1:n)

%xc Credit en bits

%xT Temps limite

%xE Temps écoulés depuis le login

%xL Temps restant

%xU Temps d'envoi

%xD Temps de réception

readme path {when {class}}

Définit le fichier dont ftpd avertira l'utilisateur de l'existence et de la dernière modification. Le paramètre when peut être LOGIN ou CWD=dir. Si when est CWD=dir, dir spécifie le nouveau répertoire par défaut qui fera afficher le message.

show-everytime {message|readme} {yes|no}

Spécifie si oui ou non le message/readme sera affiché à chaque fois que l'utilisateur change de répertoire. La valeur par défaut est non.

log commands typelist

Active l'enregistrement des commandes des utilisateurs. typelist doit être séparé par des virgules, et a pour valeur guest, anonymous ou real.

log transfers typelist direction

Active l'enregistrement des transferts de fichiers pour tous les utilisateurs réels ou anonymes. typelist doit être séparé par des virgules, et a pour valeur guest, anonymous ou real. direction est la liste, séparé par des virgules, des transferts qui doivent être enregistrés: pour les transferts sortant la valeur sera outbound et pour les transferts entrants inbound.

log security typelist

Active l'enregistrement des violations des règles de sécurités (noretrieve, .notar...) pour les utilisateurs réels, guest ou anonyme. typelist doit être séparé par des virgules, et a pour valeur guest, anonymous ou real.

log syslog

Redirige les enregistrements des transferts vers syslog. Sans cette option, les messages sont écrits dans le fichier xferlog.

incmail adress

Envoie une note lorsqu'un fichiers est envoyé au serveur.

mailfrom adress

Utilise l'adresse adress comme adresse d'expéditeur des messages concernant l'envoi de fichiers au serveur.

mailserver IP

Utilise ce serveur SMTP pour envoyer les messages sur l'envoi de fichiers au serveur. L'utilisation de plusieurs lignes de ce type permettent de changer de serveur au cas o l'un d'eux serait en panne.

alias string dir

Définit un alias, string, pour un rpertoire.

Par exemple:

alias rfc: /pub/doc/rfc

autorisera un utilisateur à accéder à /pub/doc/rfc depuis n'importe quel répertoire en utilisant la commande cd rfc:. Les alias ne fonctionnent que pour la commande cd.

cdpath dir

Définit une entrée dans le chemin des répertoires. Il définit un répertoire de

recherche lorsque l'utilisateur change répertoire.

Par exemple: `cdpath /pub/packages`

`cdpath /.aliases`

autorisera l'utilisateur à changer de répertoire dans n'importe quel répertoire sous `/pub/packages` ou sous `/.aliases`, et ce, depuis n'importe quel répertoire !

Si l'utilisateur donne la commande `cd foo`, alors le répertoire sera cherché dans:

`./foo`

`/pub/aliases/packages/foo`

`/.aliases`

Cela ne fonctionne qu'avec la commande `cd`.

include path Inclure le fichier comme faisant partie de `ftpaccess`

chmod yes|no typelist delete yes|no

typelist overwrite yes|no typelist rename yes|no

typelist umask yes|no typelist

Autorise ou interdit d'utiliser ces fonctions. Par défaut, elles sont autorisées pour tout les utilisateurs. `typelist` doit être séparé par des virgules, et a pour valeur `guest`, `anonymous` ou `real`.

passwd-check none|trivial|rfc822 (enforce|warn)

Définit le niveau de vérification du type de mot de passe pour les utilisateurs anonymes.

`none` aucun mot de passe n'est vérifié `trivial` le mot de passe doit contenir un `@`.

`rfc822` le mot de passe doit être du type défini dans le RFC822 (c'est à dire une adresse e-mail valide)

`warn` avertir l'utilisateur, mais l'autoriser à se connecter

`enforce` avertir l'utilisateur et le refuser

deny-email case-insensitive-email-address

Considère l'adresse e-mail donnée comme invalide. Si `passwd-check` a la valeur `enforced`, l'utilisateur est rejeté. Avec cette option, vous pouvez stopper les utilisateurs qui ont de stupides navigateurs WWW et qui utilisent des adresses comme `IE?0User@` ou `mozilla@`. En utilisant cela, vous ne les mettez pas dehors, mais vous les amenez peut-être à configurer correctement leur navigateur. Seulement une adresse e-mail par ligne est autorisée, mais vous pouvez utiliser plusieurs lignes `deny-email`.

upload [absolute|relative|-] root-dir dirglob

`yes|no owner group mode`

`dirs |nodirs d_mode`

Définit un répertoire avec `dirglob` qui permet ou refuse les envois. Si il permet les envois de fichiers, tous les fichiers seront la propriété de `owner` et du `group` et auront la permission `mode`.

Par exemple:

```
upload /var/ftp * no
upload /var/ftp /incoming yes ftp daemon 0666
upload /var/ftp /incoming/gifs yes jlc guest 0600 nodirs
```

Ceci autorise seulement les envois de fichiers dans /incoming et dans /incoming/gifs. Les fichiers qui seront envoyés dans /incoming auront ftp/daemon comme propriétaire et la permission 0666. Les fichiers envoyés dans /incoming/gifs auront jlc/guest comme propriétaire et la permission 0600.

Notez que root-dir doit correspondre au répertoire donné à l'utilisateur FTP dans /etc/passwd.

Vous pouvez spécifier les UID/GID numériques à la place des noms, en les faisant précéder du signe %.

Les options dirs et nodirs indiquent si la création de répertoire est autorisée. Si la création de répertoire est autorisée, l'option d_mode détermine la permission du répertoire créé. Si il est omis, le mode sera de 0777.

Le premier paramètre optionnel définit si le répertoire racine est a interpreter de fa_con relative ou absolue. Par défaut, il est interprété de fa_con absolue.

anonymous-root root-dir

root-dir spécifie le répertoire racine pour les utilisateurs anonymes. Si aucune valeur n'est donnée, l'ancienne méthode est utilisée, c'est à dire que le répertoire racine est celui donnée dans /etc/passwd.

guest-root root-dir [uid-range]

root-dir indique le répertoire racine pour les utilisateurs guest.

Si aucune valeur n'est donnée, alors le répertoire de l'utilisateur est utilisé.

Si aucun uid-range est indiqué, c'est le répertoire racine des utilisateurs guest qui ne correspondent pas à un autre critère qui sera utilisé. Plusieurs UID peuvent figurés sur une même ligne. Si un guest-root est choisi pour un utilisateur, son répertoire d'accueil sera celui de root-dir/etc/passwd et non celui de /etc/passwd du system complet. uid-range spécifie des valeurs UID numériques. L'ensemble des UID est définie par 2 nombres séparés d'un

-. Omettre le premier chiffre signifie jusqu'à, tandis qu'omettre le dernier signifie à partir de.

Par exemple:guest-root /home/users

```
guest-root /home/staff %100-999 sally
guest-root /home/users/frank/ftp frank
```

a pour cause de changer le répertoire racine vers /home/users puis d'aller dans le répertoire d'accueil spécifié dans /home/users/etc/passwd.

Les utilisateurs ayant un UID compris entre 100 et 999, inclus, et l'utilisateur sally, auront /home/staff comme répertoire racine et seront automatiquement placés dans leur répertoire d'accueil spécifié dans /home/staff/etc/passwd. L'utilisateur frank aura comme répertoire racine /home/users/owner/ftp et sera placé dans le répertoire d'accueil indiqué dans /home/users/owner/ftp/etc/passwd.

```
deny-uid uid-range [...]
deny-gid gid-range [...]
allow-uid uid-range [...]
allow-gid gid-range [...]
allow-uid et allow-gid autorisent des UID/GID qui seraient refusés avec.deny-uid
deny-gid. Ceci peut éliminer l'utilisation de /etc/ftpusers
```

Par exemple:

```
deny-gid %-99 %65535
deny-uid %-99 %65535
allow-gid ftp
allow-uid ftp
```

refuse tout accès aux utilisateurs privilégiés ou spéciaux, sauf l'utilisateur/groupe 'ftp'. Vous pouvez utiliser des noms à la place des nombres, en enlevant le signe %, évidemment...