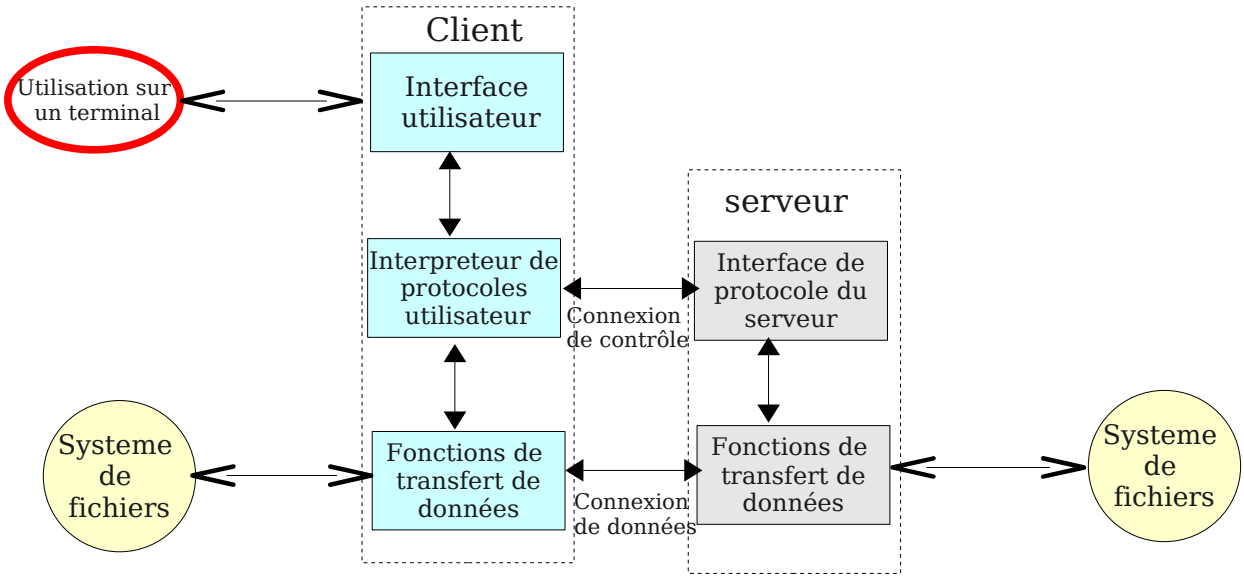
FTP

Table des matières



Client FTP en ligne de commande

Le client FTP est un logiciel qui va nous permettre de transférer des fichiers de notre ordinateur vers un serveur et réciproquement. Le client FTP est livré en standard sous Linux. Il est présent sous Windows pour peu que vous ayez installé le protocole TCP/IP.

ouvrons une console.En tapant

```
ftp alpha.poitou-charentes.iufm.fr
```

je demande à mon client ftp de se connecter au **serveur alpha.poitou-charentes.iufm.fr**

```
[etudiant@pc01]$ ftp alpha.poitou-charentes.iufm.fr

Connected to alpha.poitou-charentes.iufm.fr.

220 ProFTPD 1.2.5 Server (ProFTPD Default Installation)
[alpha.poitou-charentes.iufm.fr]

Name (alpha.poitou-charentesIufm.fr :bondazm) : anonymous
```

Le serveur me demande de m'identifier. Je veux me conecter en tant qu'anonyme donc anonymous

```
331 Anonymous login ok, send your complete email address as your password.
Password :
230 Anonymous access granted, restrictions apply.
```

Aie ! On a des droits réduits.

```
Remote system type is UNIX
```

Remote : machine distante, par opposition, local : votre station.

```
Using binary mode to transfer files.
```

Par défaut on utilise le mode binaire. Ça tombe bien on va dialoguer de unix à unix donc pas de problèmes.

Utilisation des FTP ANONYME :

Le FTP anonyme est un moyen simple de mettre des fichiers a disposition de tous (le plus souvent en lecture seule pour limiter le danger). Les serveurs FTP anonymes acceptent les connexions de n'importe qui, les authorisant a acceder aux fichiers publiques.

Autre méthode:

Entrez les commandes de connexion directement dans une console ftp:

```
ftp
open multimania.com
user tarzan
pass ********
```

Quelques commandes

ftp>

Ici le serveur FTP attends des ordres. Vous ne savez pas, alors tapez help

Ftp> help

Vous devez avoir tous les ordres possibles.

```
Ftp> ls
227 Entering Passive Mode (192,168,16,3,128,11).
150 Opening ASCII mode data connection for file list
drwxr-sr-x 2 root ftp 4096 Oct 14 21 :57 pub
226-Transfer complete.
```

ls *est le même que celui de la console. Il va vous afficher tous les répertoires et fichiers disponibles sur le serveur.*
Selon les réglages du serveur, vous pouvez tomber directement dans le répertoire "pub" ou sont rangés les fichiers qui vous intéressent auquel cas passez directement à l'étape 2 ou dans un répertoire racine du service ftp. Dans ce cas vous obtenez quatre répertoires :
bin, etc., lib : la tripaille système. C'est root sur le serveur qui gère son serveur FTP avec les infos contenues dans ces répertoires.
pub : le classique répertoire où sont stockés les fichiers disponibles.
Allons donc dans ce répertoire :

```
Ftp>cd pub
250 CWD command successful.
```

Tout c'est bien passé.

le transfert de fichiers (get *et* put)

Pour télécharger un fichier distant et le stocker sous un autre nom sur votre machine locale :
get distant-file local-file.

Pour télécharger simplement un fichier, pas besoin de spécifier un nouveau nom :
`get disant-file`.

Même chose pour envoyer un fichier de votre machine local vers le serveur :
put *local-file distant-file*.
Pour l'envoyé simplement :
`put local-file`.

lister

```
Ftp>ls
250 CWD command successful.
```
Oh joie ! Il y a pleins de fichiers.
*Il y a en particulier un mode d'em**ploi de vi qui m'intéresse.***
Ftp>**get mode_demploi_de_vi**
get *pour prendre, récupérer le fichier situé sur le serveur et le copier sur notre machine.*
```
ftp> get mode_demploi_de_vi
local : mode_demploi_de_vi remote : mode_demploi_de_vi
227 Entering Passive Mode (192,168,16,3,128,4).
150 Opening BINARY mode data connection for mode_demploi_de_vi (1681 bytes).
226 Transfer complete.
1681 bytes received in 0.0016 seconds (1e+03 Kbytes/s)
```
Nous venons de télécharger un fichier du serveur sur notre machine.

lister la machine locale

Ftp> !ls
le ! C'est pour indiquer la machine locale.

Remarques :
Refaites le téléchargement précédent: `ftp>get mode_demploi_de_vi`
Notez qu'il n'y a aucun message d'alerte, ftp écrase gentiment tout ce qui est sur sa route.

Un tas de # défilent sur l'écran

ftp>hash
Les impatients verront un tas de # défiler sur leur écran et éviteront de s'arracher les cheveux en pensant qu'il ne se passe rien.

Mettre quelque chose sur le serveur

A votre avis : un anonyme peut'il mettre quelque chose sur le serveur ?
Ceux qui ont un doute essaieront :

```
ftp> put mode_demploi_de_vi
local : mode_demploi_de_vi remote : mode_demploi_de_vi
les deux fichiers auront le même nom. C'est heureux !

227 Entering Passive Mode (192,168,16,3,128,9).
550 mode_demploi_de_vi : Permission denied
```
En tant que root, je suis rassuré. Les hostiles ne mettront pas n'importe quoi sur mon serveur.

Une petite finesse, je veux utiliser un autre répertoire sur la machine locale :
ftp>**lcd** /michel/import
l pour local, cd : pour change directory.

Maintenant tout fichier arrivera ou partira de ce répertoire.
On en a fini avec anonymous.

Se déconnecter

Ctrl-D pour se déconnecter ou quit ou exit ou bye.

ftp> bye
221 Goodbye.

On a indiqué ici qu'un nombre minimal d'ordres possibles. C'est, le minimum à savoir. Pour les accros, help vous donne tous les ordres possibles.

!	Ouvre un shell sur l'Operating System
?	Appelle le module d'aide
ascii	Configure le mode de transfert de fichiers en tant que ASCII
binary	Configure le mode de transfert de fichiers en tant que BINAIRE
cd	Change le répertoire courant sur le poste distant

close `disconnect`	Termine la connexion avec le poste distant
delete	Efface un fichier sur le poste distant
dir	Sort la liste des fichiers et répertoires présents dans le répertoire courrant sur le poste distant
get	Récupère un fichier depuis le poste distant
hash	Affiche # (dièse ou '*hash character*') pour chaque bloc de données transféré
lcd	Change le répertoire sur le poste local (localhost)
ls	Affiche la liste des fichiers et répertoires présents dans le répertoire courrant sur le poste distant
mdelete	Suppression de fichiers multiples sur le poste distant
mdir	Création d'un répertoire sur le poste distant
mget	Récupèration de fichiers multiples sur le poste distant mget *.wav mput *.gif ../images
mkdir	Création d'un répertoire sur le poste distant
mput	Emission de fichiers multiples sur le poste distant depuis le poste local.
open	Ouvre une connexion avec le poste distant
put	Emission d'un fichier vers le poste distant
pwd	Affiche le répertoire courrant sur le poste distant
quit `bye`	Termine la session FTP

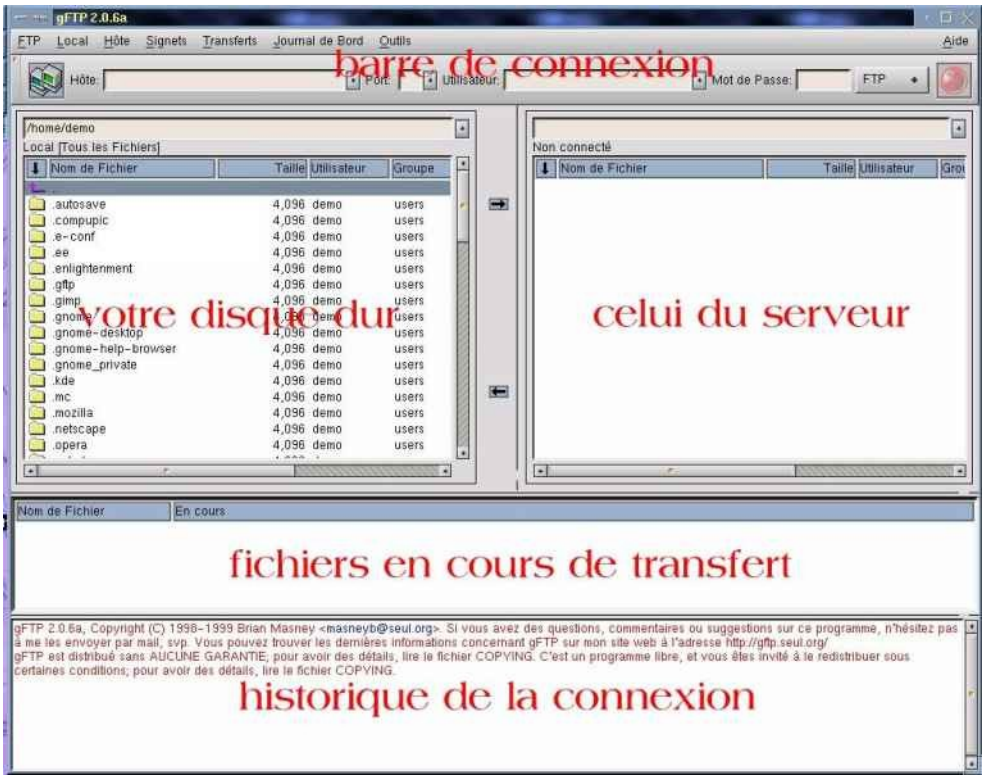
quote	Exécute une commande sur le serveur
recv	Récupère un fichier depuis le poste distant
rmdir	Supression d'un répertoire entier
send	Emission d'un fichier vers le poste distant
type	Affiche le mode courrant de transfert de fichiers (ASCII ou BYNARY)
verbose	Charge/Décharge le mode "bavard" , commencer ou arreter les prompts en texte plein
`reget`	Equivalent de `get` mais ici le transfert est reprit à la fin du fichier, pratique pour reprendre un téléchargement précédemment interrompu.

Pour les gens qui n'aiment pas taper au clavier, il existe des clients FTP en mode graphique. Apparemment plus simples ils devraient vous faciliter la tâche. Surtout que, maintenant, vous pourrez comprendre ce qui se passe.

Essayez Client FTP graphique : gFTP

Client gFTP (g pour Gnome)

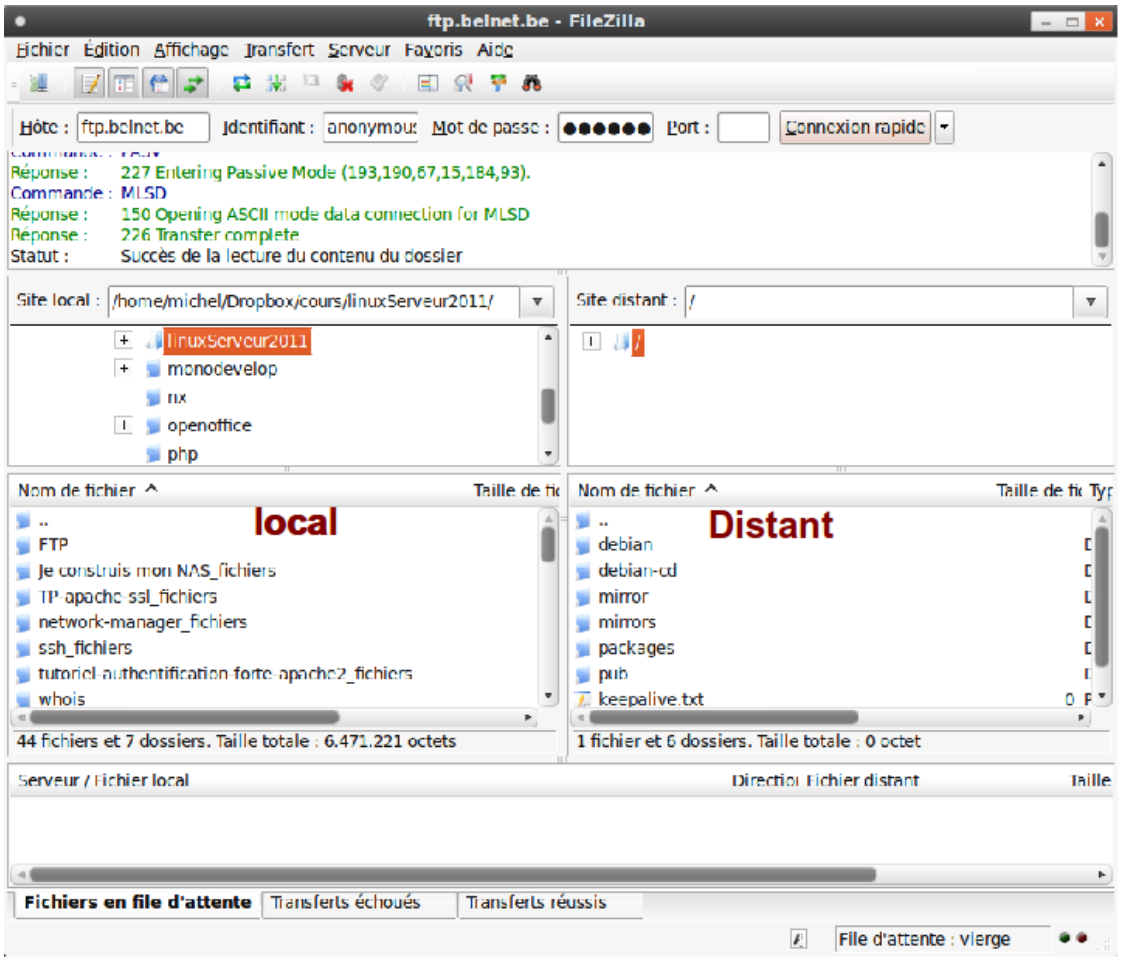
La fenêtre telle qu'elle apparaît au démarrage :



Presque le jumeau de FileZilla qui existe aussi sous linux!!!

Fillezilla

FileZilla est un logiciel FTP gratuit crée par l'allemand Tim Kosse. Il permet de se connecter à distance sur un serveur pour y télécharger des fichiers.
Un gestionnaire de site est disponible permettant de répertorier l'ensemble des adresses auxquelles vous êtes amenés à vous connecter régulièrement. Pour les besoins de sécurité, FileZilla propose un mode dans lequel il ne conserve aucune trace des mots de passe sur votre ordinateur et une authentification est nécessaire à chaque connexion aux serveurs, même en utilisant les favoris du gestionnaire de site. Le programme permet bien sûr de se connecter aux machines distantes sécurisées utilisant le protocole SSH.



L'application, gratuite et libre, est disponible en français. Ses fonctionnalités incluent le transfert de gros fichiers (plus de quatre gigas), une puissante gestion d'erreur -remplacer, renommer ou ignorer un fichier existant, par exemple-, un gestionnaire de site très complet pour ceux qui doivent fréquemment utiliser les mêmes sites, mais qui ne souhaitent pas retenir toutes les informations de connexion, ainsi que le support du glisser-déposer d'un dossier ou du bureau, bien plus rapide que la navigation.

Afin d'améliorer les vitesses de transfert, FileZilla est capable de compresser les données en cours de téléchargement. Le niveau de compression peut être ajusté selon vos besoins. Que vous téléchargiez des pages Web ou des images, le gain de temps occasionné dans la plupart des cas est considérable ! Mais dans certains cas il peut également être utile de limiter la vitesse de téléchargement pour que la totalité de la bande passante ne soit pas saturée, les vitesses de transfert de FileZilla peuvent ainsi être ajustées selon vos besoins.

FileZilla **présente une faille de sécurité critique** car il **ne crypte pas les mots de passe** enregistrés par l'utilisateur (ces informations sont enregistrées en clair dans un fichier XML situé sur le disque dur).

Depuis janvier 2010, un malware du nom de Gumblar ou Troj/JSRedir-R est capable, lorsqu'il se loge sur la machine de l'utilisateur via une faille Flash ou PDF, de récupérer les informations de connexion aux serveurs FTP enregistrés par FileZilla, puis d'y accéder afin d'injecter du code malicieux dans les fichiers de type HTML, PHP, JavaScript, ASP et ASP.NET.

vsFTPd (Very secure FTPd) : un serveur ftp ultra-sécurisé et simple

http://doc.ubuntu-fr.org/vsftpd

Installation

vsftpd est dans le dépôt Main, le nom du paquet est vsftpd pour une installation vue de Synaptic. Pour installer VsFTPd en console, entrez la commande suivante dans un terminal :

```
 apt-get install vsftpd
```

remarque :

```
vsftpd doit être lancé par un métadémon comme inetd ou xinetd. C'est un choix
délibéré de l'auteur de vsftpd de ne pas intégrer la gestion d'un mode
autonome, comme le permet ProFTPd, par exemple. Ça n'est pas particulièrement
gênant, un logiciel comme xinetd intègre toutes les fonctionnalités de contrôle
des connexions et des accès nécessaires, et un noyau moderne permet de mettre
facilement en oeuvre de la limitation de bande passante.


Dans le cas d'inetd, par exemple, une ligne comme celle-ci, ajoutée à
/etc/inetd.conf, et dans le cas où votre système fournit TCP-Wrappers, suffit :

ftp    stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/local/sbin/vsftpd

L'équivalent dans xinetd.conf serait :

service ftp
{
        socket_type     = stream
        protocol        = tcp
        wait            = no
        user            = root
        server          = /usr/local/sbin/vsftpd
}


Ensuite, veillez à ce que les utilisateurs "ftp" et "nobody" existent, avec un
répertoire pour l'utilisateur ftp, ainsi qu'un répertoire /usr/share/empty,
vide. Ces valeurs, dont nous allons constater l'utilité, pourront être
modifiées en les affinant si nécessaire dans la configuration.
```

Configuration de vsftpd

La configuration de VsFTPd est centralisée dans un seul et même fichier `/etc/vsftpd.conf`.

Par défaut la configuration standard interdit tout ou presque, c'est à vous et seulement avec quelques lignes de configuration de définir quelles seront les capacités et les accès autorisés ou interdits à l'utilisateur.

Étudions-la de plus près. Le fichier de configuration fourni dans la

distribution source de vsftpd, **vsftpd.conf**, que vous devez avoir placé dans /etc, est très court une fois toutes les lignes commentées et les explications dissimulées :

```
[~/vsftpd-1.0.1]$ egrep -v '^(#|$)' vsftpd.conf
anonymous_enable=YES
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
```

- `anonymous_enable` autorise l'accès anonyme au serveur (comportement par défaut) sur le répertoire /var/ftp ou /home/ftp (debian) de l'utilisateur ftp dans le fichier passwd.
- `dirmessage_enable` active l'affichage des fichiers .message à l'entrée dans les répertoires.
- `xferlog_enable` active un journal des téléchargements.
- `connect_from_port_20` active l'utilisation du port source 20 pour les PORT.

Les trois dernières directives ne sont là que pour outrepasser le comportement par défaut du serveur, et le rendre un petit peu plus traditionnel, mais il est amusant de remarquer que vsftpd est parfaitement capable de fonctionner en tant que serveur FTP à accès anonyme en lecture uniquement, avec un fichier de configuration entièrement vide.

Un fichier plus utile:

```
listen=YES
anonymous_enable=YES
local_enable=YES #Pour permettre à vos utilisateurs locaux
write_enable=YES #(ceux qui ont un compte sur la machine) de se connecter au serveur
                 #      et d'écrire.
local_umask=077     #Pour permettre la configuration du chmod par défaut
                    # que prendront les fichiers et les dossiers.
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES #Vous pouvez « emprisonner » certains utilisateurs
                      # dans leur dossier personnel
```

umask:

1. Valeur 002 : droit des dossiers en 775 et fichiers en 664
2. Valeur 022 : droits des dossiers en 755 et fichiers en 644
3. Valeur 077 : droits des dossiers en 777 et fichiers en 666

Vous pouvez personnaliser le texte de connexion au serveur

```
ftpd_banner=Bienvenue sur le serveur ftp de jojo
```

Vous pouvez « emprisonner » certains utilisateurs dans leur dossier personnel grâce à la configuration suivante : chroot_local_user=YES

Après chaque changement sur la configuration, pensez à relancer (ou reconfigurer) le serveur pour les prendre en compte :

```
sudo /etc/init.d/vsftpd restart (ou reload)
```

Un autre fichier "standard" de configuration de vsFTPd :

anonymous_enable=NO	connexion en tant qu'anonyme interdite
local_enable=YES	connexion pour les utilisateurs locaux autorisés
write_enable=NO	écriture interdite
anon_upload_enable=NO	Upoad pour anonyme interdit
anon_mkdir_write_enable=NO	création de répertoire pour les anonymes interdit
anon_other_write_enable=NO	écriture de fichier pour anonyme interdit
chroot_local_user=YES	enferme l'utilisateur dans le répertoire ftp (chrooté)
per_source = 5	nombre de connexions maximales autorisées par une même adresse IP
no_access = 192.168.1.3	interdiction de se connecter au ftp à partir de cette adresse
guest_enable=YES	Rend possible la connexion d'utilisateurs virtuels
guest_username=virtual	souhaitable, vu que la connexion anonyme est refusée
pasv_min_port=30000	cette option permet de limiter l'accès des ports
pasv_max_port=30999	disponibles, utile derrière un firewall
xferlog_enable=YES	enregistrement des logs...

simple et court

En fait,'on ne pouvais pas mettre un nom DNS
dans pasv_address=XX.XX.XX.XX.
en mettant l'IP publique tout ok.
Pour les étourdis comme moi, ne pas oublier d'avoir dans la génération du certificat le même le Common name = l'hôte dns et pas autre chose...

Dans le man de vsftpd et dans la conf par défaut, rien ne fait allusion à cette MAGNIFIQUE et INDISPENSABLE directive :
pasv_addr_resolve=YES

En effet, elle permet d'indiquer à vsftpd de résoudre l'adresse IP en nom d'hôte, ce qu'il ne fait pas par défaut.

Un répertoire commun aux utilisateurs

http://blog.pastoutafait.org/billets/Configuration-de-VsFTPd-sous-Ubuntu

Il peut être intéressant de mettre en place un répertoire commun aux utilisateurs, pour faire cela, il faut créer un utilisateur, disons "partage" :

```
sudo adduser partage
```

Puis indiquer correctement les droits:

```
$ sudo chmod -R 755 /home/partage
$ sudo chown partage:partage -R /home/partage
```

Créer ensuite un répertoire "/home/utilisateur/partage" dans le dossier personnel de chaque utilisateur, puis modifier le fichier /etc/fstab pour "mounter" automatiquement le répertoire partagé dans les "home" des utilisateurs.

```
$ mkdir /home/utilisateur/partage
$ sudo chown utilisateur:utilisateur /home/utilisateur/partage
```

> $ chown user.group fichier
>
> Même si cette méthode est encore supportée, c'est avec un ':' qu'il devrait être utilisé puisqu'il est possible d'avoir des utilisateurs avec des '.'.
>
> chown permet de faire
>
> ```
> $chown user: fichier
> ```
>
> Cela permet de changer le user et le groupe en même temps tout en utilisant le groupe principal (celui défini dans /etc/passwd) de l'utilisateur donné.

```
$ sudo chmod 755 /home/utilisateur/partage
```

```
$ sudo nano /etc/fstab
```

Et y ajouter une ligne
`/home/partage /home/utilisateur/partage auto bind,defaults 0 0`
pour chaque utilisateur.

Et voilà, tout les utilisateurs disposeront d'un répertoire "partage" commun.
Pour allez plus loin, il peut aussi être intéressant de disposer d'un répertoire commun accessible en écriture. Pour cela, il suffit de créer un répertoire dans le "home" de l'utilisateur "partage", et de lui donner les droits adéquates:

```
$ sudo mkdir /home/partage/upload
$ sudo chown partage:partage /home/partage/upload
$ sudo chmod 777 /home/partage/upload
```

remarques sur bind :

Utiliser l'option « bind » avec la commande « mount »

Après avoir monté un disque, par exemple dans /media/disque-test, il peut être intéressant de monter l'intégralité du contenu, ou un répertoire seulement, de ce disque dans un autre répertoire sans démonter /media/disque-test.

Cela permet par exemple :

- de « recopier » ce contenu dans un répertoire tout spécialement destiné à un partage FTP,
- un utilisateur qui n'a pas accès au disque-test par le répertoire de montage peut ainsi se voir conférer des droits d'accès à un sous répertoire du disque-test s'il a accès au répertoire lié (le répertoire lié et les fichiers qu'il contient doivent autoriser cet accès)

Cela est possible avec l'option "bind" (bind signifie lier en anglais) de la commande « mount » qui s'utilise ainsi en ligne de commande :

```
mount --bind /media/répertoire-à-lier /home/user/répertoire-lié
mount --bind /source-"privée"-à-rendre-visible /répertoire-accessible-à-tous
sudo mount --bind /media/disque/répertoire /home/user/répertoire-lié
```

Pour faire perdurer ces montages, il faut alors spécifier ce montage dans le fichier fstab.

Éditez le fichier **/etc/fstab**.

On indique le montage 'bind' de la façon suivante : '/media/disque/répertoire /home/user/répertoire-lié none bind 0 0'

Voici un exemple :

```
# /etc/fstab: static file system information.
#
# file system   mount point     type         options                    dump  pass
proc            /proc           proc         defaults                   0     0
/dev/hda2       /               ext3         defaults,errors=remount-ro 0     1
/dev/hda3       /home           ext3         defaults                   0     2
/dev/hda6       /media/stock    ext3         defaults                   0     2
/dev/hda1       /media/win_c    vfat         defaults,umask=0           0     0
/dev/hda7       /media/win_d    vfat         defaults,umask=0           0     0
/dev/hdb1       /media/windows  ntfs         ro,uid=1000,gid=1000       0     2
/dev/hda8       /media/debian   reiserfs     defaults                   0     2
/dev/hda5       none            swap         sw                         0     0
/dev/hdc        /media/cdrom0   udf,iso9660  ro,user,noauto             0     0

# mes répertoires liés
/media/Maxtor1 /home/user/Maxtor1 none bind 0 0
```

Il suffit de retirer le dernier paragraphe du fichier fstab pour annuler l'opération au prochain redémarrage.

Serveur avec utilisateurs virtuels

voir

http://www.andesi.org/reseau/vsftpd-un-serveur-ftp-securise-et-simple

Configurer le serveur ProFTP

Une petite doc:http://www.brakstar.com/forum/braktopic_108.html

`#apt-get install proftpd proftpd-mysql` (*si vos avez l'intention d'utiliser mysql)*

choisissez de lancer le service proftpd en mode « Stand alone »

vérifiez en tapant ftp localhost

```
[michel@bureau michel]$ ftp localhost
Connected to localhost.
220 ProFTPD 1.2.5 Server (ProFTPD Default Installation)
[bureau.perso]
500 AUTH not understood.
500 AUTH not understood.
KERBEROS_V4 rejected as an authentication type
Name (localhost:michel): michel
331 Password required for michel.
Password:
230 User michel logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
ftp> cd /
250 CWD command successful.
ftp> ls
227 Entering Passive Mode (127,0,0,1,128,12).
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 root     root            0 Nov 15 10:18 1
drwxr-xr-x   2 root     root         4096 Nov 15 10:06 bin
drwxr-xr-x   3 root     root         4096 Jan 12 11:04 boot
drwxr-xr-x   1 root     root            0 Jan  1  1970 dev
drwxr-xr-x  60 root     root         4096 Jan 12 11:04 etc
drwxr-xr-x   4 root     root         4096 Dec  9 15:38 home
drwxr-xr-x   2 root     root         4096 Nov 15 09:36 initrd
drwxr-xr-x   9 root     root         4096 Dec 16 14:32 lib
drwxr-xr-x  12 root     root         4096 Dec 29 17:58 mnt
drwxr-xr-x   3 root     root         4096 Nov 22 18:49 opt
dr-xr-xr-x 116 root     root            0 Jan 12 12:02 proc
drwxrwxrwx   3 root     root         4096 Nov 18 14:27 public
drwx------  16 root     root         4096 Jan 10 13:45 root
drwxr-xr-x   2 root     root         4096 Dec 16 14:32 sbin
drwxrwxrwt  92 root     root         4096 Jan 12 11:07 tmp
drwxr-xr-x  12 root     root         4096 Nov 22 18:52 usr
drwxr-xr-x  20 root     root         4096 Nov 15 09:57 var
226-Transfer complete.
226 Quotas off
```

```
ftp>
ftp> bye
221 Goodbye.
```

Deux défauts 'apparaissent :

- Les "anonymes" ne peuvent pas se connecter à notre serveur
- Les clients authentifiés peuvent se balader partout

Il faut donc les régler.

Le paramètrage.

Commencons par créer un double du fichier original que nous allons trafiquer.
Le fichier qui nous interesse est : **/etc/proftpd.conf**

Faites en un double que vous nommerez proftpd.conf.original.
Lancer un éditeur de texte et ouvrez proftpd.conf

Recherchez cette ligne

```
...
DenyFilter      \*.*/
...
```

Ajoutez la ligne suivante juste après

```
DefaultRoot      ~
```

enregistrez le fichier et redémarrez le service par la commande suivante

```
sudo /etc/init.d/proftpd restart
```

Les anonymes

Tout ce que nous avons à faire ici est de créer la section anonymous pour que les clients puissent se connecter en anonymous.

```
<Anonymous ~ftp>
  User                ftp
  Group               nogroup
  # les anonymes se connectent en « anonymous ou ftp »
  UserAlias           anonymous ftp
  # Cosmetic changes, all files belongs to ftp user
  DirFakeUser  on ftp
  DirFakeGroup on ftp

  RequireValidShell       off
```

```
  # Limit the maximum number of anonymous logins
  MaxClients                10

  # We want 'welcome.msg' displayed at login, and '.message' displayed
  # in each newly chdired directory.
  DisplayLogin              welcome.msg
  DisplayFirstChdir           .message

  # Limit WRITE everywhere in the anonymous chroot
  <Directory *>
    <Limit WRITE>
      DenyAll
    </Limit>
  </Directory>
</Anonymous>
```

L'utilisateur anonymous sera un alias du compte ftp, 10 connexions maxi, sans shell de commande, sans mot de passe valide, sans droit d'écriture.

Les authentifiés

On limite la capacité de navigation des utilisateurs authentifiés à leur seul répertoire. Le réglage par défaut leur permet en effet d'aller se ballader partout dans l'arborescence.

C'est à la dernière ligne : **DefaultRoot ~**

Le ~ indique le répertoire utilisateur.

On dit que l'utilisateur a été "**chrooté**" (changement de racine)
chroot remplace le répertoire racine du processus en cours par celui spécifié par le chemin . Ce répertoire sera utilisé comme origine des chemins commençant par /. Le répertoire racine est hérité par tous les enfants du pro cessus ayant fait le changement.

Vous devez avoir un fichier proftpd.conf qui ressemble à ça :

```
# 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              "ProFTPD Sur linux"
 ServerType              standalone
 DefaultServer           on
 # Allow FTP resuming.
 # Remember to set to off if you have an incoming ftp for upload.
 AllowStoreRestart           on
 # 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.
 Umask     022
 # 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
 # Normally, we want files to be overwriteable.
 <Directory /*>
  AllowOverwrite on
 </Directory>
 # Needed for NIS.
 PersistentPasswd  off
 <Anonymous ~ftp>
 User ftp
 Group ftp
 UserAlias anonymous ftp
 MaxClients 10
 RequireValidShell off
 AnonRequirePassword off
 <Limit WRITE>
 DenyAll
 </Limit>
 </Anonymous>
 # Default root can be used to put users in a chroot environment.
 # As an example if you have a user foo and you want to put
 # foo in /home/foo
 # chroot environment you would do this:
 # DefaultRoot /home/foo foo
 Defaultroot ~
```

Enregistrez.

relancez le démon.
Pour ce faire, ouvrez une console et tapez
[root@pc_mic root]# **/etc/init.d/proftpd** ***Attention, la ligne complète !!***

La machine m'indique quelles options sont disponibles.
Status : pour savoir si le démon est actif ou non.
Start ou Stop : sans commentaires

Nous allons utiliser ici **restart**
[root@pc_mic root]# **/etc/rc.d/init.d/proftpd restart**

Le démon s'arrête puis redémarre en tenant compte des nouveaux réglages.
N'oubliez pas de faire cette manoeuvre après chaque modification du fichier de configuration.

Les anonymes peuvent maintenant se connecter. Ils ne pourront rien faire tant que vous n'aurez pas mis à leur disposition des fichiers dans le répertoire **/var/ftp/pub**. N'oubliez pas de changer les droits ! Il est rare que root aime voir ses fichiers se balader dans la nature.

Vous pouvez à tout moment voir qui est connecté à votre serveur avec la commande

```
ftpwho
```

et voir les statistiques avec :

```
ftpstats
```

Vous pouvez malgré tout utiliser une interface graphique pour gérer proftpd.

Elle se nomme gproftpd.