Logiciel

Pro-ftpd : un serveur FTP open source pour Linux

Introduction

ProFTPD est un serveur FTP/SFTP/FTPS open source, modulaire et puissant.

- Il gère les répertoires cachés, les hôtes virtuels et les fichiers **.ftpaccess** par répertoire.
- La structure interne des répertoires anonymes FTP est quelconque (pas besoin de bin, lib ni de fichiers spéciaux).
- Il gère les fonctionnalités avancées (plusieurs fichiers de mots de passe, ratios téléchargement/envoi, etc.).

Pré-requis

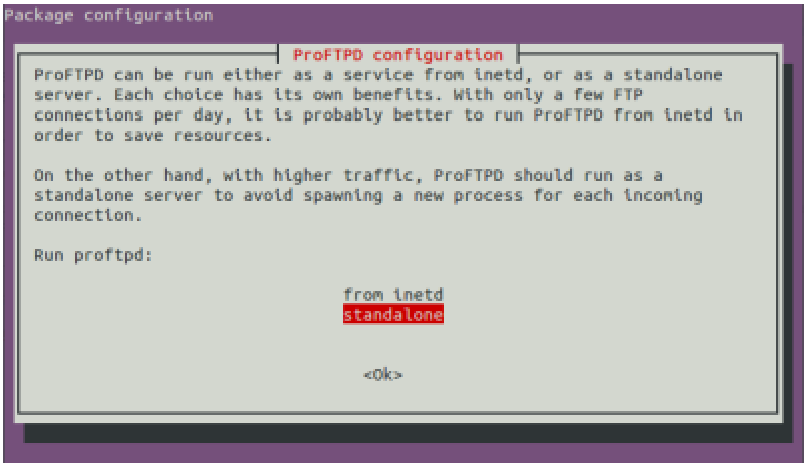
Installation

Pour utiliser une authentification sur une base de données, installez les paquets **proftpd-mod** suggérés correspondants.

1. Installez les paquets **proftpd,ftp** ou (cas d'un Raspberry Pi) :

   ```
   ...@...:~$ sudo apt install proftpd ftp
   ```

   - **ftp** pour les tests
   - Lors de l’installation, il peut vous être demandé comment ProFTP doit être démarré. Choisissez **autonome** (**standalone**) :



```
ProFTPD can be run either as a service from inetd, or as a standalone
server. Each choice has its own benefits. With only a few FTP
connections per day, it is probably better to run ProFTPD from inetd in
order to save resources.

On the other hand, with higher traffic, ProFTPD should run as a
standalone server to avoid spawning a new process for each incoming
connection.

Run proftpd:

                    from inetd
                    standalone

                       <Ok>
```

   - Vous pouvez installer aussi les paquets **proftpd-mod-ldap,proftpd-mod-mysql,proftpd-mod-odbc,proftpd-mod-pgsql,proftpd-mod-sqlite,proftpd-mod-geoip** ou

```
...@...:~$ sudo apt install proftpd-mod-ldap proftpd-mod-mysql proftpd-mod-odbc proftpd-mod-pgsql proftpd-mod-sqlite proftpd-mod-geoip
```

   - L'installation crée les utilisateurs système suivants :
      - **proftpd** (UID 127), groupe **nogroup** ; pas de répertoire personnel **/run/proftpd**.
      - **ftp** (UID 128), groupe **nogroup** ; création du répertoire personnel **/srv/ftp** »…

2. Vérifiez que ftp fonctionne sous l'utilisateur en cours (**pi** pour un Raspberry Pi) :

```
...@...:~$ ftp localhost
...
Name (localhost:xxxxxxx):
331 Mot de passe requis pour xxxxxxx
Password:
230 Utilisateur xxxxxxx authentifié
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
...
drwxrwxr-x   4 xxxxxxx  xxxxxxx      4096 Sep  5 05:39 Bureau
...
226 Téléchargement terminé
ftp> bye
221 Au revoir.
...@...:~$
```

3. Si vous essayez avec un client comme **Filezilla**, vous constaterez que l'utilisateur n'est pas bloqué dans son home.

Configuration

- L'installation a créé l’arborescence :

```
...@...:~$ tree -d /etc/proftpd/
/etc/proftpd/
└── conf.d
```

ou pour un Raspberry Pi :

```
pi@framboise:~ $ tree -d
/etc/proftpd/
/etc/proftpd/
└── conf.d
```

- **Pour le listing des fichiers de la distribution**, voir ProFTPd : Fichiers de la distribution

- Pour que les réglages persistent après les mises à jour, nous ne toucherons pas au fichier **/etc/proftpd/proftpd.conf**.
- Nous placerons dans le répertoire **/etc/proftpd/conf.d/** des fichiers contenant nos directives de configuration. Ces fichiers ne seront pas affectés par les mises à jour.
- Liste des directives : http://www.proftpd.org/docs/directives/linked/by-name.html

Utilisateurs virtuels

Chaque utilisateur a accès à son propre répertoire personnel **/home/xxxxxxx** (ou **/home/pi** pour un Raspberry Pi).

- Unix ne connaît que les UID : il n'utilise pas les noms d'utilisateurs.
- **proftpd** ne fait donc pas de différence entre un utilisateur système et un utilisateur virtuel : ils sont définis par leur UID.
- Un **utilisateur virtuel** est un utilisateur qui n'est pas défini dans le système.

Création d'un webmestre pour un site monsite.tld

Nous allons créer un utilisateur virtuel **admiweb** pour accéder par ftp au site **monsite.tld**, hébergé à l'emplacement **/var/www/html/monsite.tld**

1. Vérifiez l'existence de l'utilisateur **www-data** et de son groupe :

   ```
   ...@...:~$ id www-data
   uid=33(www-data) gid=33(www-data) groupes=33(www-data)
   ```

   → L’identifiant du groupe **www-data** est **33**.

   - Si le groupe **www-data** n'existe pas, créez-le ainsi que l'utilisateur **www-data** par :

     ```
     ...@...:~$ sudo groupadd www-data
     ...@...:~$ sudo useradd -g www-data -d /var/www -s
     /bin/false www-data
     ```

2. Créez un nouvel utilisateur virtuel ayant accès à **/var/www/html** (le webmestre **admiweb**, de home **/var/www/html**, avec les uid et gid de **www-data**, fournissez et confirmez le **mot de passe** du nouveau compte) :

   ```
   ...@...:~$ cd /etc/proftpd/
   ...@...:/etc/proftpd$ sudo ftpasswd --passwd --name admiweb --
   gid 33 --uid 33 --home /var/www/html --shell /bin/false
   ftpasswd: creating passwd entry for user admiweb
   ...
   Password:
   Re-type password:
   ...
   ftpasswd: entry created
   ```

Création d'un utilisateur virtuel (cas général)

On peut créer de la même façon des utilisateurs virtuels ayant des identifiants quelconques (sauf UID 0 (zéro) et GID 0 (zéro) qui sont utilisés pour l'utilisateur root et le groupe root).

Utilisez pour les utilisateurs virtuels des identifiants qui ne sont pas déjà utilisés dans **/etc/passwd** pour séparer les privilèges de vos utilisateurs système de ceux de vos utilisateurs virtuels.

Les privilèges sont déterminés par les identifiants.

Les utilisateurs virtuels peuvent tous avoir les mêmes identifiants → ils auront tous exactement les mêmes privilèges.

La directive **DefaultRoot ~** dans **/etc/proftpd/conf.d/global.conf** confine vos utilisateurs virtuels dans des répertoires personnels distincts.

Ainsi, ces utilisateurs virtuels, bien qu'ayant tous les mêmes privilèges, seront tous séparés dans des répertoires différents.

L'outil ftpasswd est un script Perl.

Fichier de configuration

1. Créez ou éditez avec les droits d'administration le fichier **/etc/proftpd/conf.d/global.conf** pour ajouter à la fin votre configuration :

   /etc/proftpd/conf.d/global.conf

   ```
   # Tous les utilsateurs seront emprisonnés dans leur home, sauf l'utilisateur système xxxxxxx
   DefaultRoot ~ !xxxxxxx

   # Pas de shell valide exigé (ex : bin/sh ou /bin/bash).
   RequireValidShell off

   # Fichier des mots de passe
   AuthUserFile /etc/proftpd/ftpd.passwd

   # Fichier des groupes
   AuthGroupFile /etc/proftpd/ftpd.group

   AuthOrder mod_auth_file.c  mod_auth_unix.c
   AuthPAM off
   ```

   Cas d'un Raspberry Pi :

   /etc/proftpd/conf.d/global.conf

   ```
   # Tous les utilsateurs seront emprisonnés dans leur home, sauf l'utilisateur système pi
   DefaultRoot ~ !pi

   # Pas de shell valide exigé (ex : bin/sh ou /bin/bash).
   RequireValidShell off

   # Fichier des mots de passe
   AuthUserFile /etc/proftpd/ftpd.passwd

   # Fichier des groupes
   AuthGroupFile /etc/proftpd/ftpd.group
   ```

```
AuthOrder mod_auth_file.c  mod_auth_unix.c
AuthPAM off
```

2. Créez les fichiers **/etc/proftpd/ftp.passwd** et **/etc/proftpd/ftpd.group** :

```
...@...:~$ sudo touch /etc/proftpd/ftp.passwd
...@...:~$ sudo touch /etc/proftpd/ftpd.group
```

Rechargement et test

1. Relancez proftpd et vérifiez que l'utilisateur admiweb peut se connecter :
2. Relancez proftpd et vérifiez que l'utilisateur admiweb peut se connecter :

```
...@...:~$ sudo systemctl restart proftpd
...@...:~$ ftp localhost
...
Name (localhost:xxxxxxx): admiweb
331 Mot de passe requis pour admiweb
Password:
230 Utilisateur admiweb authentifié
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
...
-rwxrws---   1 admiweb  www-data      612 Apr 25  2018
index.nginx-debian.html
...
ftp> bye
221 Au revoir.
...@...:~$
```

Pour un Raspberry Pi :

```
pi@framboise:~ $ sudo systemctl restart proftpd
pi@framboise:~ $ ftp localhost
Connected to localhost.
220 ProFTPD Server (Debian) [::1]
Name (localhost:pi): admiweb
331 Mot de passe requis pour admiweb
Password:
230 Utilisateur admiweb authentifié
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
...
drwxrws---  22 admiweb  www-data     4096 Jul 28 13:23
html
...
ftp> bye
```

```
221 Au revoir.
pi@framboise:~ $
```

3. L'utilisateur système xxxxxxx, lui, peut se connecter et n'est pas emprisonné :

```
...@...:~$ ftp localhost
...
Name (localhost:xxxxxxx):
331 Mot de passe requis pour xxxxxxx
Password:
230 Utilisateur xxxxxxx authentifié
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
...
drwxrwxr-x   4 xxxxxxx  xxxxxxx      4096 Sep  5 05:39 Bureau
...
226 Téléchargement terminé
ftp> cd ..
...
ftp> ls
...
drwxrwxr-x 269 xxxxxxx  xxxxxxx     20480 Sep 10 11:51 xxxxxxx
...
ftp> bye
221 Au revoir.
...@...:~$
```

Pour un Raspberry Pi :

```
pi@framboise:~ $ ftp localhost
...
Name (localhost:pi):
331 Mot de passe requis pour pi
Password:
230 Utilisateur pi authentifié
...
ftp> ls
...
drwxr-xr-x   2 pi       pi           4096 Sep  9 16:15 Desktop
...
ftp> cd ..
...
ftp> ls
...
drwxr-xr-x  33 pi       pi           4096 Sep  9 17:53 pi
```

```
...
ftp> bye
221 Au revoir.
pi@framboise:~ $
```

Fichier proftpd.conf et dérivés

Il inclut :

- **/etc/proftpd/modules.conf**
  - Répertoire des modules DSO : /usr/lib/proftpd
  - Seul l'utilisateur root peut charger et décharger des modules, mais tout le monde peut voir quels modules ont été chargés.
  - Charge les modules mod_ctrls_admin.c, mod_tls.c, mod_radius.c, mod_quotatab.c, mod_quotatab_file.c, mod_quotatab_radius.c, mod_wrap.c, mod_rewrite.c, mod_load.c, mod_ban.c, mod_wrap2.c, mod_wrap2_file.c, mod_dynmasq.c, mod_exec.c, mod_shaper.c, mod_ratio.c, mod_site_misc.c, mod_sftp.c, mod_sftp_pam.c, mod_facl.c, mod_unique_id.c, mod_copy.c, mod_deflate.c, mod_ifversion.c, mod_tls_memcache.c, mod_ifsession.c

2. **/etc/proftpd/conf.d/**
3. (désactivés) :
   - #/etc/proftpd/ldap.conf (entièrement désactivé par des #)
   - #/etc/proftpd/sql.conf (entièrement désactivé par des #)
   - #/etc/proftpd/tls.conf (entièrement désactivé par des #)
   - #/etc/proftpd/virtuals.conf (entièrement désactivé par des #)

Après chaque changement de configuration, pensez à relancer proftpd :

```
$ sudo systemctl restart proftpd
```

Sécurisation TLS

Le serveur est maintenant en place, cependant, tout ce qui transite entre votre serveur et votre Client FTP transite en clair sur le Net.

Nous allons chiffrer le tout avec une sécurisation TLS (SSLv3 étant deprecated).

Commençons par créer un certificat SSL auto-signé :

```
$ sudo openssl req -new -x509 -days 365 -nodes -out
/etc/ssl/certs/proftpd.cert -keyout
/etc/ssl/private/proftpd.key

Generating a 2048 bit RSA private key
.........................................................
.+++
.........................................................
.........................+++
writing new private key to '/etc/ssl/private/proftpd.key'
-----
You are about to be asked to enter information that will
be incorporated
into your certificate request.
What you are about to enter is what is called a
Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:sd-
xxxxx.dedibox.fr
Email Address []:me@mymail.tld
```

Renseignez les champs demandés avec les bonnes informations. (sd-xxxxx.dedibox.fr : votre nom de domaine si vous en avez un).

Protégez la clé :

```
$ sudo chmod 440 /etc/ssl/private/proftpd.key
```

Nous allons maintenant forcer notre serveur FTP à utiliser cette clé pour générer une connexion chiffrée.

Avec les droits d'administration, éditez le fichier **/etc/proftpd/conf.d/tls.conf** pour le modifier comme ceci :

/etc/proftpd/conf.d/tls.conf

```
<IfModule mod_tls.c>
  TLSEngine on
  TLSLog /var/log/proftpd/tls.log

  # TLSv1 Uniquement
  TLSProtocol TLSv1
```

```
    # N'autorise que les connexions sécurisées
    TLSRequired on

    # Renseigne l'emplacement des certificats
    TLSRSACertificateFile
/etc/ssl/certs/proftpd.cert
    TLSRSACertificateKeyFile
/etc/ssl/private/proftpd.key

    TLSVerifyClient off
    TLSRenegotiate none
    TLSOptions NoSessionReuseRequired

  </IfModule>
```

Redémarrez le serveur FTP :

```
$ sudo systemctl restart proftpd
```

Vous pouvez maintenant vous connecter à votre serveur FTP de manière sécurisée !

Quelques exemples de fichiers de configuration

- **Basic** :

Basic.conf

basic.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          "ProFTPD Default
Installation"
ServerType          standalone
DefaultServer           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 under which the server
will run.
User                nobody
Group               nogroup

# To cause every FTP user to be "jailed"
(chrooted) into their home
# directory, uncomment this line.
#DefaultRoot ~

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

# A basic anonymous configuration, no upload
directories.  If you do not
# want anonymous users, simply delete this
entire <Anonymous> section.
<Anonymous ~ftp>
  User              ftp
  Group             ftp

  # We want clients to be able to login with
"anonymous" as well as "ftp"
  UserAlias         anonymous ftp

  # 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
  <Limit WRITE>
    DenyAll
  </Limit>
</Anonymous>
```

- **Anonymous**

anonymous.conf

anonymous.conf

```
# This sample configuration file illustrates
configuring two
# anonymous directories, and a guest (same thing
as anonymous but
# requires a valid password to login)

ServerName          "ProFTPD Anonymous Server"
ServerType          standalone

# Port 21 is the standard FTP port.
Port                21

# If you don't want normal users logging in at
all, uncomment this
# next section
#<Limit LOGIN>
#  DenyAll
#</Limit>

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

# 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 maximum number of seconds a data
connection is allowed
# to "stall" before being aborted.
TimeoutStalled          300

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

# Our "basic" anonymous configuration, including
a single
# upload directory ("uploads")
<Anonymous ~ftp>

  # Allow logins if they are disabled above.
  <Limit LOGIN>
    AllowAll
  </Limit>

  # Maximum clients with message
  MaxClients            5 "Sorry, max %m users -
- try again later"

  User              ftp
  Group             ftp
  # We want clients to be able to login with
"anonymous" as well as "ftp"
  UserAlias         anonymous ftp

  # Limit WRITE everywhere in the anonymous
chroot
  <Limit WRITE>
    DenyAll
  </Limit>

  # An upload directory that allows storing
files but not retrieving
  # or creating directories.
  <Directory uploads/*>
    <Limit READ>
      DenyAll
    </Limit>

    <Limit STOR>
      AllowAll
    </Limit>
  </Directory>
</Anonymous>
```

```
# A second anonymous ftp section.  Users can
login as "private".  Here
# we hide files owned by root from being
manipulated in any way.

<Anonymous /usr/local/private>
  User              bobf
  Group             users
  UserAlias         private bobf
  UserAlias         engineering bobf

  # Deny access from *.evil.net and
*.otherevil.net, but allow
  # all others.
  <Limit LOGIN>
    Order           deny,allow
    Deny            from .evil.net,
.otherevil.net
    Allow           from all
  </Limit>

  # We want all uploaded files to be owned by
'engdept' group and
  # group writable.
  GroupOwner            engdept
  Umask             006

  # Hide all files owned by user 'root'
  HideUser          root

  <Limit WRITE>
    DenyAll
  </Limit>

  # Disallow clients from any access to hidden
files.
  <Limit READ DIRS>
    IgnoreHidden            on
  </Limit>

  # Permit uploading and creation of new
directories in
  # submissions/public

  <Directory submissions/public>
    <Limit READ>
      DenyAll
      IgnoreHidden          on
    </Limit>

    <Limit STOR MKD RMD XMKD XRMD>
```

```
      AllowAll
      IgnoreHidden          on
    </Limit>
  </Directory>
</Anonymous>

# The last anonymous example creates a "guest"
account, which clients
# can authenticate to only if they know the
user's password.

<Anonymous ~guest>
  User                  guest
  Group                 nobody
  AnonRequirePassword       on

  <Limit LOGIN>
    AllowAll
  </Limit>

  # Deny write access from all except trusted
hosts.
  <Limit WRITE>
    Order               allow, deny
    Allow               from 10.0.0.
    Deny                from all
  </Limit>
</Anonymous>
```

- **Simple MySQL Authentication**

mysql_simple.conf

mysql_simple.conf

```
##
## Config with simple mysql authentication
support
## Contributed by 'Stonki'
## Added to www.proftpd.org 18/Oct/2002
##

# This is a basic ProFTPD configuration file. It
establishes a single
# server and a single anonymous login. It
assumes that you have a
# user/group "nobody"/"nogroup" for normal
operation and anon.

#    !!! PLEASE read the documentation of
```

```
proftpd !!!
#
# You can find the documentation in
/usr/doc/packages/proftpd/,
# http://www.proftpd.org/ and don't forget to
read carefully
# and _follow_ hints on
http://www.proftpd.net/security.html.


#
# geaendert: 03.11.2001 für ProFTP 1.2.4 und
mod_sql 4.x
#

#
# Basic
#
ServerName          "Stonki"
serverType          inetd
ServerAdmin         support@stonki.de

#
# Debug Level
# emerg, alert, crit (empfohlen), error, warn.
notice, info, debug
#
#SyslogLevel            emerg
#SystemLog          /var/log/proftpd.system.log

#
# uncomment, if you want to hide the servers
name:
#
ServerIdent         on    "Stonki's Server"
DeferWelcome            on
DefaultServer           on

#
# Display
#
DisplayLogin            /messages/ftp.motd
DisplayConnect          /net/messages/ftp.pre
DisplayFirstChdir       index.txt

HiddenStor          off
DirFakeUser         on stonki
DirFakeGroup            on stonki
DirFakeMode         0000

# Enable PAM for authentication...
```

```
#
AuthPAM             on

# Setting this directive to on will cause
authentication to fail
# if PAM authentication fails. The default
setting, off, allows
# other modules and directives such as
AuthUserFile and friends
# to authenticate users.
#
# AuthPAMAuthoritative      on

# This directive allows you to specify the PAM
service name used
# in authentication (default is "proftpd" on
SuSE Linux).
# You have to setup the service in the
/etc/pam.d/<other_name>.
#
#AuthPAMConfig          <other_name>

# Port 21 is the standard FTP port.
Port                21

#------------------------mysql Modul: 4.x
#
# Zugangskontrolle
#
SQLAuthTypes            Plaintext
SQLAuthenticate         users*
SQLConnectInfo          db@localhost username
password
SQLDefaultGID           65534
SQLDefaultUID           65534
SQLMinUserGID           100
SQLMinUserUID                   500
SQLUserInfo         ftp username password uid
gid homedir shell

#
# aktive SQL Kommandos, ab hier passiert etwas
:-)
#
SQLLog PASS counter
SQLNamedQuery counter UPDATE
"letzter_zugriff=now(), count=count+1 WHERE
username='%u'" ftp

# xfer Log in mysql
SQLLog RETR,STOR transfer1
```

```
SQLNamedQuery  transfer1 INSERT "'%u', '%f',
'%b', '%h', '%a', '%m', '%T', now(), 'c', NULL"
xfer_stat

SQLLOG ERR_RETR,ERR_STOR transfer2
SQLNamedQuery  transfer2 INSERT "'%u', '%f',
'%b', '%h', '%a', '%m', '%T', now(), 'i', NULL"
xfer_stat

#------------------------mysql

# Port 21 is the standard FTP port.
Port                            21

# disable listen on 0.0.0.0:21 - the port (and
IP) should
# be specified explicitly in each VirtualHost
definition
#
#Port                           0

# listen for each (additional) address
explicitly that is
# specified (via Bind and Port) in a VirtualHost
definition
#
#SocketBindTight        on

#
# FXP Unterstuetzung
#
AllowForeignAddress         on


# Umask 022 is a good standard umask to prevent
new dirs
# and files from being group and world writable.
Umask               022

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

# Maximal Werte setzen
MaxClientsPerHost   3    "Nicht mehr als %m
Verbindungen"
MaxClients      5     "Leider sind schon %m
Clients verbunden"

# RateReadBPS             5000
# RateReadFreeBytes       5000
# RateReadHardBPS         on

Classes on
Class default           limit 5
Class internet          limit 2
Class local             limit 3
Class internet          ip 0.0.0.0/0
Class internet      ip 192.168.99.99/24
Class local             ip 127.0.0.1/24
Class local             ip 192.168.0.0/24

#
# Restart erlauben
#
AllowStoreRestart               on
AllowRetrieveRestart                on

# Normally, we want files to be overwriteable.
<Directory /*>
    AllowOverwrite             off
    HideNoAccess            on
    <Limit READ>
     AllowAll
    </Limit>
    <Limit Write>
     DenyAll
    </Limit>
</Directory>

<Directory /net/incoming/*>
        AllowOverwrite   on
    <Limit STOR CMD MKD WRITE>
     AllowALL
    </Limit>
    <Limit RETR DELE>
     DenyALL
    </Limit>
</Directory>


# It is a very good idea to allow only filenames
containing normal
# alphanumeric characters for uploads (and not
shell code...)
#PathAllowFilter "^[a-zA-Z0-9_.-]()'+$"
#PathAllowFilter "^[a-zA-Z0-9 _.-]()'+$"

# We don't want .ftpaccess or .htaccess files to
be uploaded
#PathDenyFilter "(\.ftp)|(\.ht)[a-z]+$"
```

```
#PathDenyFilter "\.ftp[a-z]+$"

# Do not allow to pass printf-Formats (security!
see documentation!):
#AllowFilter "^[a-zA-Z0-9@~ /,_.-]*$"
#DenyFilter  "%"

# 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

# Performance: skip DNS resolution when we
process the logs...
UseReverseDNS               on

# Turn off Ident lookups
IdentLookups                on

# Set the maximum number of seconds a data
connection is allowed
# to "stall" before being aborted.
TimeoutStalled                  300

# Where do we put the pid files?
ScoreboardPath          /usr/local/var/proftpd

#
# Logging options
#
TransferLog
/var/log/proftpd.xferlog

# Some logging formats
#
LogFormat            default "%h %l %u %t \"%r\"
%s %b"
LogFormat            auth    "%v [%P] %h %t
\"%r\" %s"
LogFormat            write   "%h %l %u %t \"%r\"
%s %b"

# Log file/dir access
```

```
ExtendedLog
/var/log/proftpd.access_log    WRITE,READ write

# Record all logins
ExtendedLog
/var/log/proftpd.auth_log      AUTH auth

# Paranoia logging level....
ExtendedLog
/var/log/proftpd.paranoid_log  ALL default

#
# Do a chroot for web-users (i.e. public or www
group), but
# do not change root if the user is also in the
users group...
#
DefaultRoot  ~       !users

#
# Limit login attempts
#
MaxLoginAttempts                3

#
# Users needs a valid shell
#
RequireValidShell               off
```

- **Virtual hosts**

virtual.conf

virtual.conf

```
# This sample configuration file illustrates
creating two
# virtual servers, and associated anonymous
logins.

ServerName          "ProFTPD"
ServerType          inetd

# Port 21 is the standard FTP port.
Port                21

# Global creates a "global" configuration that
is shared by the
# main server and all virtualhosts.

```

```
<Global>
  # Umask 022 is a good standard umask to
prevent new dirs and files
  # from being group and world writable.
  Umask             022
</Global>

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

# 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

# Maximum seconds a data connection may "stall"
TimeoutStalled          300

# First virtual server
<VirtualHost ftp.virtual.com>
  ServerName            "Virtual.com's FTP
Server"

  MaxClients            10
  MaxLoginAttempts      1

  # DeferWelcome prevents proftpd from
displaying the servername
  # until a client has authenticated.
  DeferWelcome          on

  # Limit normal user logins, because we only
want to allow
  # guest logins.
  <Limit LOGIN>
    DenyAll
  </Limit>

  # Next, create a "guest" account (which could
be used
  # by a customer to allow private access to
their web site, etc)
  <Anonymous ~cust1>
    User            cust1
    Group           cust1
    AnonRequirePassword     on

    <Limit LOGIN>
      AllowAll
    </Limit>

    HideUser            root
    HideGroup           root

    # A private directory that we don't want the
user getting in to.
    <Directory logs>
      <Limit READ WRITE DIRS>
        DenyAll
      </Limit>
    </Directory>
  </Anonymous>
</VirtualHost>

# Another virtual server, this one running on
our primary address,
# but on port 4000.  The only access is to a
single anonymous login.
<VirtualHost our.ip.address>
  ServerName            "Our private FTP server"
  Port              4000
  Umask             027

  <Limit LOGIN>
    DenyAll
  </Limit>

  <Anonymous /usr/local/ftp/virtual/a_customer>
    User            ftp
    Group           ftp
    UserAlias           anonymous ftp

    <Limit LOGIN>
      AllowAll
    </Limit>

    <Limit WRITE>
      DenyAll
    </Limit>

    <Directory incoming>
      <Limit WRITE>
```

```
        AllowAll
      </Limit>
    </Directory>
  </Anonymous>
</VirtualHost>
```

- **Complex Virtual**

virtual_authuserfile.conf

virtual_authuserfile.conf

```
#
# Virtual Hosting Server Configuration
# by M.Lowes <markl@ftech.net>
# for Frontier Internet Services Limited
#      (http://www.ftech.net/)
#
ServerName          "Master Webserver"
#
# Spawn from inetd?
#
#ServerType         inetd
#
# or maybe a standalone server...
#
ServerType          standalone
#
# don't give the server banner until _after_ authentication
#
DeferWelcome            off
#
# Some basic defaults
#
Port                  21
Umask                002
TimeoutLogin         120
TimeoutIdle          600
TimeoutNoTransfer    900
TimeoutStalled      3600
#
# No, I don't think we'll run as root!
#
User                ftp
Group               ftp
#
# This is a non-customer usable name, (ie they should be connecting via www.{domain})
# not 'hostname'.  Therefore let's dump them in
```

```
a dummy account and wait for them to
# scream.
#
DefaultRoot         /web/Legacy/
#
# Performance, let's do DNS resolution when we
process the logs...
#
UseReverseDNS        off
#
# Where do we put the pid files?
#
ScoreboardPath          /var/run/proftpd
#
# Logging options
#
TransferLog
/var/spool/syslog/proftpd/xferlog.legacy
#
# Some logging formats
#
LogFormat         default "%h %l %u %t \"%r\" %s
%b"
LogFormat           auth    "%v [%P] %h %t
\"%r\" %s"
LogFormat           write   "%h %l %u %t \"%r\"
%s %b"
#
# Global settings
#
<Global>
    DisplayLogin           welcome.msg
    DisplayFirstChdir       readme
    #
    # having to delete before uploading is a
pain ;)
    #
    AllowOverwrite           yes
    #
    # Turn off Ident lookups
    #
    IdentLookups         off
    #
    # Logging
    #
    # file/dir access
    #
    ExtendedLog
/var/spool/syslog/proftpd/access.log WRITE,READ
write
    #
    #
    # Record all logins
    #
    ExtendedLog
/var/spool/syslog/proftpd/auth.log AUTH auth
    #
    # Paranoia logging level....
    #
   ##ExtendedLog
/var/spool/syslog/proftpd/paranoid.log ALL
default
</Global>

#
# Deny writing to the base server...
#
<Limit WRITE>
    DenyAll
</Limit>


# ----------------------------------------------
# Virtual Servers start here....
#
# (Note: this is normally auto generated by a
# script written in house).
# ----------------------------------------------
#
# www.ftech.net.
# This is the default server
# Gets all the connections for
www.{customer.domain},
# & www.ftech.net
#
<VirtualHost www.ftech.net>
    ServerAdmin        webmaster@Ftech.net
    ServerName        "Master Webserver"
    MaxLoginAttempts    2
    RequireValidShell    no
    TransferLog
/var/spool/syslog/proftpd/xferlog.www
    MaxClients        50
    DefaultServer        on
    DefaultRoot        ~ !staff
    AllowOverwrite        yes

    #
    # No quickly do we kick someone out
    #
    TimeoutLogin            120
    TimeoutIdle            600
    TimeoutNoTransfer        900

    # ------------------------------------------
--
    # Got a Frontpage customer who keeps
breaking things????
    #  - stick 'em in group fpage
    # ------------------------------------------
--
    <Directory ~/public_html>
    #
    # Block them from doing anything other than
reading...
    #
        <Limit STOR RNFR DELE>
            DenyGroup fpage
        </Limit>
    </Directory>
    #
    # ditto for ftp_root if it's there...
    #
    <Directory ~/ftp_root>
        <Limit STOR RNFR DELE>
            DenyALL
        </Limit>
    </Directory>
    #
    # Limit by IP...
    #
    <Directory /web/zsl>
        <Limit ALL>
            Order Allow,Deny
            Allow 195.200.31.220
            Allow 212.32.17.0/26
            Deny ALL
        </Limit>
    </Directory>

</VirtualHost>

# ---------------------------------------------
#
# Legacy server, left in because some people
# haven't realised it's gone yet.  Shove 'em
into
# a dummy $home
#
<VirtualHost web-1.ftech.net>
ServerAdmin     webmaster@Ftech.net
ServerName      "Legacy Web Upload Server"
MaxLoginAttempts    2
```

```
RequireValidShell   no
MaxClients      50
DefaultRoot     ~ !staff
MaxClients      2
AllowOverwrite      yes
TransferLog
/var/spool/syslog/proftpd/xferlog.web-1
</VirtualHost>

# --------------------------------------------
#
# ftp.ftech.net
#
<VirtualHost ftp.ftech.net>
ServerAdmin         ftpmaster@ftech.net
ServerName          "Frontier Internet Public
FTP Server"
TransferLog         /ftp/xferlog/ftp.ftech.net
MaxLoginAttempts        3
RequireValidShell       no
DefaultRoot         /ftp/ftp.ftech.net
AllowOverwrite          yes

#
# Auth files....
#
AuthUserFile
/var/conf/ftp/authfiles/passwd.ftp.ftech.net
AuthGroupFile
/var/conf/ftp/authfiles/group.ftp.ftech.net

# A basic anonymous configuration, no upload
directories.
<Anonymous /ftp/ftp.ftech.net>
    User            ftp
    Group            ftp
    # We want clients to be able to login with
"anonymous" as well as "ftp"
    UserAlias        anonymous ftp
    RequireValidShell        no

    # Limit the maximum number of anonymous
logins
    MaxClients        50

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

    <Directory pub/incoming>
        <Limit STOR>
```

```
            AllowAll
        </Limit>
        <Limit WRITE DIRS READ>
            DenyAll
        </Limit>
        <Limit CWD XCWD CDUP>
            AllowAll
        </Limit>
    </Directory>

    <Directory home>
        <Limit ALL>
            DenyAll
        </Limit>
    </Directory>

   #
   # Limit access to the mirrors to LINX
   # only
   #
   <Directory mirrors>
      <Limit RETR>
         Order Allow,Deny
         Allow .uk, .ftech.net
         Allow .vom.tm
         Deny ALL
      </Limit>
   </Directory>

    # Limit WRITE everywhere in the anonymous
chroot
    <Limit WRITE>
            DenyAll
    </Limit>


</Anonymous>

</VirtualHost>

# ----------------------------------------------
------
# Virtual ftp with anon access, but no incoming
#
<VirtualHost ftp.foo1.com>
ServerAdmin             ftpmaster@foo1.com
ServerName              "Foo1 FTP Server"
TransferLog
/var/spool/syslog/xfer/ftp.foo1.com
MaxLoginAttempts        3
RequireValidShell       no
```

```
DefaultRoot             /ftp/ftp.foo1.com
User                    foo1
Group                   foo1
AllowOverwrite          yes

#
# Auth files....
#
AuthUserFile
/var/conf/ftp//authfiles/passwd.ftp.foo1.com
AuthGroupFile
/var/conf/ftp//authfiles/group.ftp.foo1.com

<Anonymous /ftp/ftp.foo1.com>
        User                    ftp
        Group                   ftp
        UserAlias               anonymous ftp
        RequireValidShell       no
        MaxClients              20
    <Limit WRITE>
        DenyAll
    </Limit>
</Anonymous>
</VirtualHost>


# -----------------------------------------------
------
# ftp.foo2.com
# Anon, no incoming, some private access areas
#
<VirtualHost ftp.foo2.com>
ServerAdmin
ftpmaster@mcresearch.co.uk
ServerName              "MC Research FTP Server"
TransferLog
/var/spool/syslog/xfer/ftp.foo2.com
MaxLoginAttempts        3
RequireValidShell       no
DefaultRoot             /ftp/ftp.foo2.com
User                    foo2
Group                   foo2
AllowOverwrite          yes

#
# Auth files....
#
AuthUserFile
/var/conf/ftp//authfiles/passwd.ftp.foo2.com
AuthGroupFile
/var/conf/ftp//authfiles/group.ftp.foo2.com
```

```
<Anonymous /ftp/ftp.foo2.com>
        User                    ftp
        Group                   ftp
        UserAlias               anonymous ftp
        RequireValidShell       no
        MaxClients              20

    <Directory download>
        <Limit ALL>
            DenyAll
        </Limit>
    </Directory>
    <Limit WRITE>
        DenyAll
    </Limit>
</Anonymous>

    <Directory /ftp/ftp.foo2.com/pub>
        <Limit WRITE>
            AllowUser mcres
            DenyAll
        </Limit>
    </Directory>

    <Directory /ftp/ftp.foo2.com/download>
        <Limit ALL>
            AllowUser mcres
            AllowUser customer
            DenyAll
        </Limit>
    </Directory>
</VirtualHost>


# ------------------------------------------------
------
# ftp.foo3.com
#
#
<VirtualHost ftp.foo3.com>
ServerAdmin             ftpmaster@farrukh.co.uk
ServerName              "Farrukh FTP Archive"
TransferLog
/var/spool/syslog/xfer/ftp.foo3.com
MaxLoginAttempts        3
RequireValidShell       no
DefaultRoot             /web/farrukh2/ftp_root
User                    farrukh2
Group                   farrukh2
AllowOverwrite          yes
```

```
#
# Auth files....
#
AuthUserFile
/var/conf/ftp//authfiles/passwd.ftp.foo3.com
AuthGroupFile
/var/conf/ftp//authfiles/group.ftp.foo3.com

<Anonymous /web/farrukh2/ftp_root>
        User                    ftp
        Group                   ftp
        UserAlias               anonymous ftp
        RequireValidShell       no
        MaxClients              20

    <Directory pub/incoming/*>
        <Limit STOR>
            AllowAll
        </Limit>
        <Limit WRITE DIRS READ>
            DenyAll
        </Limit>
        <Limit CWD XCWD CDUP>
            AllowAll
        </Limit>
    </Directory>


    <Directory pub/Incoming/*>
        <Limit STOR>
            AllowAll
        </Limit>
        <Limit WRITE DIRS READ>
            DenyAll
        </Limit>
        <Limit CWD XCWD CDUP>
            AllowAll
        </Limit>
    </Directory>
    #
    # block access to the secure areas by
anon...
    #
    <Directory fpub>
        <Limit ALL>
            DenyAll
        </Limit>
    </Directory>

    <Directory fgroup>
        <Limit ALL>
```

```
            DenyAll
        </Limit>
    </Directory>
    <Limit WRITE>
        DenyAll
    </Limit>
</Anonymous>

    #
    # define user based access
    #
    <Directory /web/farrukh2/ftp_root/fpub>
        <Limit ALL>
            AllowUser farrukh
            AllowUser fguest
            DenyAll
        </Limit>
    </Directory>

    <Directory /web/farrukh2/ftp_root/fgroup>
        <Limit ALL>
            AllowUser farrukh
            AllowUser fgroup
            DenyAll
        </Limit>
    </Directory>
</VirtualHost>


# ----------------------------------------------
------
# ftp.foo4.com
# anon, with incoming upload
#
<VirtualHost ftp.foo4.com>
ServerAdmin             ftpmaster@teamwork.co.uk
ServerName              "Teamwork FTP Server"
TransferLog
/var/spool/syslog/xfer/ftp.foo4.com
MaxLoginAttempts        3
RequireValidShell       no
DefaultRoot             /ftp/ftp.foo4.com
User                    foo4
Group                   foo4
AllowOverwrite          yes

#
# Auth files....
#
AuthUserFile
/var/conf/ftp//authfiles/passwd.ftp.foo4.com
```

```
AuthGroupFile
/var/conf/ftp//authfiles/group.ftp.foo4.com

<Anonymous /ftp/ftp.foo4.com>
        User                    ftp
        Group                   ftp
        UserAlias               anonymous ftp
        RequireValidShell       no
        MaxClients              20

    <Directory pub/incoming/*>
        <Limit STOR>
            AllowAll
        </Limit>
        <Limit WRITE DIRS READ>
            DenyAll
        </Limit>
        <Limit CWD XCWD CDUP>
            AllowAll
        </Limit>
    </Directory>


    <Directory pub/Incoming/*>
        <Limit STOR>
            AllowAll
        </Limit>
        <Limit WRITE DIRS READ>
            DenyAll
        </Limit>
        <Limit CWD XCWD CDUP>
            AllowAll
        </Limit>
    </Directory>

    <Limit WRITE>
        DenyAll
    </Limit>
</Anonymous>
</VirtualHost>

# ----------------------------------------------
------
# The end....
# ----------------------------------------------
------
```

Fichier /etc/proftpd/proftpd.conf

- **Fichier Proftpd.conf exemple**

Proftpd.conf

Proftpd.conf

```
# Fichier de configuration de ProFTPD
#   Pour une liste complète des directives :
http://www.proftpd.org/docs/directives/configuration_full.html
#   /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
#   To really apply changes, reload proftpd after modifications, if
#   it runs in daemon mode. It is not required in inetd/xinetd mode.

# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 on

# Virtualhosts
#   Emplacement du fichier contenant la liste des utilisateurs virtuels,
AuthUserFile /etc/proftpd/ftpd.passwd
#   Emplacement du fichier contenant la liste des groupes virtuels,
AuthGroupFile /etc/proftpd/ftpd.group

# Active l'utilisation du fichier /etc/ftpusers qui donne la liste des utilisateur n'ayant pas d'accès au serveur ftp
#    ( fichier ftpusers situé dans /etc ).
UseFtpUsers on

# If set on you can experience a longer connection delay in many cases.
IdentLookups off

# Nom du serveur FTP
ServerName "Debian"

# Mode de fonctionnement du serveur ( inetd ou standalone )
ServerType standalone
DeferWelcome off
MultilineRFC2228 on

# Si vous utilisez des virtualhosts, laissez
```

```
cette option activée, sinon désactivez la.
DefaultServer on
ShowSymlinks on

# Déconnection du client au bout de "x" secondes
# S'il n'opère aucun transfert.
TimeoutNoTransfer 600

# S'il a stoppé le transfert.
TimeoutStalled 600

# S'il n'a effectué aucune activité après la
saisie du login/passwd.
TimeoutIdle 1200

DisplayLogin
DisplayChdir
ListOptions
welcome.msg
.message true
"-l"
DenyFilter
\*.*/
# Permet de "chrooter" les utilisateurs FTP
locaux dans leurs répertoires personnels.Ici
tous les utilsateurs seront
« emprisonnés » sauf l'utilisateur mickael,
DefaultRoot
~ !mickael
#Si cette directive est mise sur "on" , proftpd
exigera que les utilisateurs qui se connectent
aient des shells valides ( ex :
bin/sh ou /bin/bash ).
RequireValidShell
on
#Port d'écoute du serveur ftp.
Port
21#Plage des ports passifs que ProFTPd utilisera
pour répondre aux clients,
# PassivePorts
49152 65534
# If your host was NATted, this option is useful
in order to
# allow passive tranfers to work. You have to
use your public
# address and opening the passive ports used on
your firewall as well.
# MasqueradeAddress
1.2.3.4
# This is useful for masquerading address with
dynamic IPs:
```

```
# refresh any configured MasqueradeAddress
directives every 8 hours
<IfModule mod_dynmasq.c>
# DynMasqRefresh 28800
</IfModule>
#Nombre maximal de connexions simultanées.
MaxInstances
30
# Définit avec quel utilisateur/groupe ProFTPD
sera lancé ( vous pouvez modifier le nom de
l'utilisateur ou bien le groupe
comme vous le voulez )
User
userftp
Group
groupftp
# Umask 022 is a good standard umask to prevent
new files and dirs
# (second parm) from being group and world
writable.
#Droits du propriétaire du fichier 022 donnes
des droits 664 ( rw-r--r-- ) pour les fichiers
et 755 ( rwxr-xr-x ) pour les
dossiers.
Umask
022 022
#Si la directive est mise à "on" cela permettra
de remplacer les anciens fichiers par les
nouveaux, cette option sera inutile
si vous interdisez l'écriture.
AllowOverwrite
on
# Uncomment this if you are using NIS or LDAP
via NSS to retrieve passwords:
# PersistentPasswd
off
# This is required to use both PAM-based
authentication and local passwords
# AuthOrder
mod_auth_pam.c* mod_auth_unix.c
# Be warned: use of this directive impacts CPU
average load!
# Uncomment this if you like to see progress and
transfer rate with ftpwho
# in downloads. That is not needed for uploads
rates.
#
# UseSendFile
off
#Emplacement du fichier log pour les transferts.
TransferLog /var/log/proftpd/xferlog
```

```
#Emplacement du fichier log du serveur FTP.
SystemLog /var/log/proftpd/proftpd.log
# Logging onto /var/log/lastlog is enabled but set to off by default
#UseLastlog on
# In order to keep log file dates consistent after chroot, use timezone info
# from /etc/localtime. If this is not set, and proftpd is configured to
# chroot (e.g. DefaultRoot or <Anonymous>), it will use the non-daylight
# savings timezone regardless of whether DST is in effect.
#SetEnv TZ :/etc/localtime
<IfModule mod_quotatab.c>
QuotaEngine off
</IfModule>
<IfModule mod_ratio.c>Ratios off
</IfModule>
# Delay engine reduces impact of the so-called Timing Attack described in
# http://www.securityfocus.com/bid/11430/discuss
# It is on by default.
<IfModule mod_delay.c>
DelayEngine on
</IfModule>
<IfModule mod_ctrls.c>
ControlsEngine off
ControlsMaxClients 2
ControlsLog /var/log/proftpd/controls.log
ControlsInterval 5
ControlsSocket /var/run/proftpd/proftpd.sock
</IfModule>
<IfModule mod_ctrls_admin.c>
AdminControlsEngine off
</IfModule>
#
# Alternative authentication frameworks
#
#Include /etc/proftpd/ldap.conf
#Include /etc/proftpd/sql.conf
#
# This is used for FTPS connections
#
#Include /etc/proftpd/tls.conf
#
# Useful to keep VirtualHost/VirtualRoot
```

```
directives separated
#
#Include /etc/proftpd/virtuals.conf
# A basic anonymous configuration, no upload
directories.
#Configuration du mode anonyme.Si vous voulez
autoriser ce mode, décommenter toutes les
lignes,
# <Anonymous ~ftp>
# User
ftp
# Group
nogroup
# # We want clients to be able to login with
"anonymous" as well as "ftp"
# UserAlias
anonymous ftp
# # Cosmetic changes, all files belongs to ftp
user
# DirFakeUseron 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
# DisplayChdir
.message
#
# # Limit WRITE everywhere in the anonymous
chroot
# <Directory *># <Limit WRITE>
#
DenyAll
# </Limit>
# </Directory>
#
# # Uncomment this if you're brave.
# # <Directory incoming>
# # # Umask 022 is a good standard umask to
prevent new files and dirs
# # # (second parm) from being group and world
writable.
```

```
# # Umask
022 022
# #
<Limit READ WRITE>
# #
DenyAll
# #
</Limit>
# #
<Limit STOR>
# #
AllowAll
# #
</Limit>
# # </Directory>
#
# </Anonymous>
Partie SSL/TLS
<IfModule mod_tls.c>
# Activation du SSL
TLSEngine on
# On force toutes les connections avec ssl
TLSRequired on
# logs
TLSLog /var/log/proftpd/proftpd.tls_log
# Protocole
TLSProtocol SSLv23
# Pas de demande de certificat client
TLSOptions NoCertRequest
# Certificat et clé
TLSRSACertificateFile
/etc/ssl/certs/proftpd.cert.pem
TLSRSACertificateKeyFile
/etc/ssl/certs/proftpd.key.pem
# Pas de vérification du certificat client
TLSVerifyClient off
</IfModule>
# Include other custom configuration files
Include /etc/proftpd/conf.d/
```

Modèle de fichier proftpd.conf

proftpd.conf

```
# Fichier de configuration de ProFTPD
#   Pour une liste complète des directives :
http://www.proftpd.org/docs/directives/configura
tion_full.html
# /etc/proftpd/proftpd.conf -- This is a basic
```

```
ProFTPD configuration file.
# To really apply changes, reload proftpd after
modifications, if it runs in daemon mode.
# It is not required in inetd/xinetd mode.
#
# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is
annoying on IPv4 only boxes.
UseIPv6 on

#Virtualhosts

#Emplacement du fichier contenant la liste des
utilisateurs virtuels,
AuthUserFile /etc/proftpd/ftpd.passwd

#Emplacement du fichier contenant la liste des
groupes virtuels,
AuthGroupFile /etc/proftpd/ftpd.group

#Active l'utilisation du fichier /etc/ftpusers
qui donne la liste des utilisateur n'ayant pas
d'accès au serveur ftp ( fichier
ftpusers situé dans /etc ).
UseFtpUsers on

# If set on you can experience a longer
connection delay in many cases.
IdentLookups
off
# Nom du serveur FTP
ServerName
"Debian"
#Mode de fonctionnement du serveur ( inetd ou
standalone )
ServerType
standalone
DeferWelcome
off
MultilineRFC2228
on
#Si vous utilisez des virtualhosts, laissez
cette option activée, sinon désactivez la.
DefaultServer
on
ShowSymlinks
on
# Déconnection du client au bout de "x" secondes
#S'il n'opère aucun transfert.
```

```
TimeoutNoTransfer
600
#S'il a stoppé le transfert.
TimeoutStalled
600
#S'il n'a effectué aucune activité après la
saisie du login/passwd.
TimeoutIdle
1200
DisplayLogin
DisplayChdir
ListOptions
welcome.msg
.message true
"-l"
DenyFilter
\*.*/
# Permet de "chrooter" les utilisateurs FTP
locaux dans leurs répertoires personnels.Ici
tous les utilsateurs seront
« emprisonnés » sauf l'utilisateur mickael,
DefaultRoot
~ !mickael
#Si cette directive est mise sur "on" , proftpd
exigera que les utilisateurs qui se connectent
aient des shells valides ( ex :
bin/sh ou /bin/bash ).
RequireValidShell
on
#Port d'écoute du serveur ftp.
Port
21#Plage des ports passifs que ProFTPd utilisera
pour répondre aux clients,
# PassivePorts
49152 65534
# If your host was NATted, this option is useful
in order to
# allow passive tranfers to work. You have to
use your public
# address and opening the passive ports used on
your firewall as well.
# MasqueradeAddress
1.2.3.4
# This is useful for masquerading address with
dynamic IPs:
# refresh any configured MasqueradeAddress
directives every 8 hours
<IfModule mod_dynmasq.c>
# DynMasqRefresh 28800
</IfModule>
#Nombre maximal de connexions simultanées.
```

```
MaxInstances
30
# Définit avec quel utilisateur/groupe ProFTPD
sera lancé ( vous pouvez modifier le nom de
l'utilisateur ou bien le groupe
comme vous le voulez )
User
userftp
Group
groupftp
# Umask 022 is a good standard umask to prevent
new files and dirs
# (second parm) from being group and world
writable.
#Droits du propriétaire du fichier 022 donnes
des droits 664 ( rw-r--r-- ) pour les fichiers
et 755 ( rwxr-xr-x ) pour les
dossiers.
Umask
022 022
#Si la directive est mise à "on" cela permettra
de remplacer les anciens fichiers par les
nouveaux, cette option sera inutile
si vous interdisez l'écriture.
AllowOverwrite
on
# Uncomment this if you are using NIS or LDAP
via NSS to retrieve passwords:
# PersistentPasswd
off
# This is required to use both PAM-based
authentication and local passwords
# AuthOrder
mod_auth_pam.c* mod_auth_unix.c
# Be warned: use of this directive impacts CPU
average load!
# Uncomment this if you like to see progress and
transfer rate with ftpwho
# in downloads. That is not needed for uploads
rates.
#
# UseSendFile
off
#Emplacement du fichier log pour les transferts.
TransferLog /var/log/proftpd/xferlog
#Emplacement du fichier log du serveur FTP.
SystemLog /var/log/proftpd/proftpd.log
# Logging onto /var/log/lastlog is enabled but
set to off by default
#UseLastlog on
# In order to keep log file dates consistent
```

```
after chroot, use timezone info
# from /etc/localtime. If this is not set, and
proftpd is configured to
# chroot (e.g. DefaultRoot or <Anonymous>), it
will use the non-daylight
# savings timezone regardless of whether DST is
in effect.
#SetEnv TZ :/etc/localtime
<IfModule mod_quotatab.c>
QuotaEngine off
</IfModule>
<IfModule mod_ratio.c>Ratios off
</IfModule>
# Delay engine reduces impact of the so-called
Timing Attack described in
# http://www.securityfocus.com/bid/11430/discuss
# It is on by default.
<IfModule mod_delay.c>
DelayEngine on
</IfModule>
<IfModule mod_ctrls.c>
ControlsEngine
off
ControlsMaxClients 2
ControlsLog
/var/log/proftpd/controls.log
ControlsInterval
5
ControlsSocket
/var/run/proftpd/proftpd.sock
</IfModule>
<IfModule mod_ctrls_admin.c>
AdminControlsEngine off
</IfModule>
#
# Alternative authentication frameworks
#
#Include /etc/proftpd/ldap.conf
#Include /etc/proftpd/sql.conf
#
# This is used for FTPS connections
#
#Include /etc/proftpd/tls.conf
#
# Useful to keep VirtualHost/VirtualRoot
directives separated
#
#Include /etc/proftpd/virtuals.conf
# A basic anonymous configuration, no upload
directories.
#Configuration du mode anonyme.Si vous voulez
```

```
autoriser ce mode, décommenter toutes les
lignes,
# <Anonymous ~ftp>
# User
ftp
# Group
nogroup
# # We want clients to be able to login with
"anonymous" as well as "ftp"
# UserAlias
anonymous ftp
# # Cosmetic changes, all files belongs to ftp
user
# DirFakeUseron 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
# DisplayChdir
.message
#
# # Limit WRITE everywhere in the anonymous
chroot
# <Directory *># <Limit WRITE>
#
DenyAll
# </Limit>
# </Directory>
#
# # Uncomment this if you're brave.
# # <Directory incoming>
# # # Umask 022 is a good standard umask to
prevent new files and dirs
# # # (second parm) from being group and world
writable.
# # Umask
022 022
# #
<Limit READ WRITE>
# #
DenyAll
```

```
# #
</Limit>
# #
<Limit STOR>
# #
AllowAll
# #
</Limit>
# # </Directory>
#
# </Anonymous>
Partie SSL/TLS
<IfModule mod_tls.c>
# Activation du SSL
TLSEngine on
# On force toutes les connections avec ssl
TLSRequired on
# logs
TLSLog /var/log/proftpd/proftpd.tls_log
# Protocole
TLSProtocol SSLv23
# Pas de demande de certificat client
TLSOptions NoCertRequest
# Certificat et clé
TLSRSACertificateFile
/etc/ssl/certs/proftpd.cert.pem
TLSRSACertificateKeyFile
/etc/ssl/certs/proftpd.key.pem
# Pas de vérification du certificat client
TLSVerifyClient off
</IfModule>
# Include other custom configuration files
Include /etc/proftpd/conf.d/
```

Autre exemple

proftpd.conf

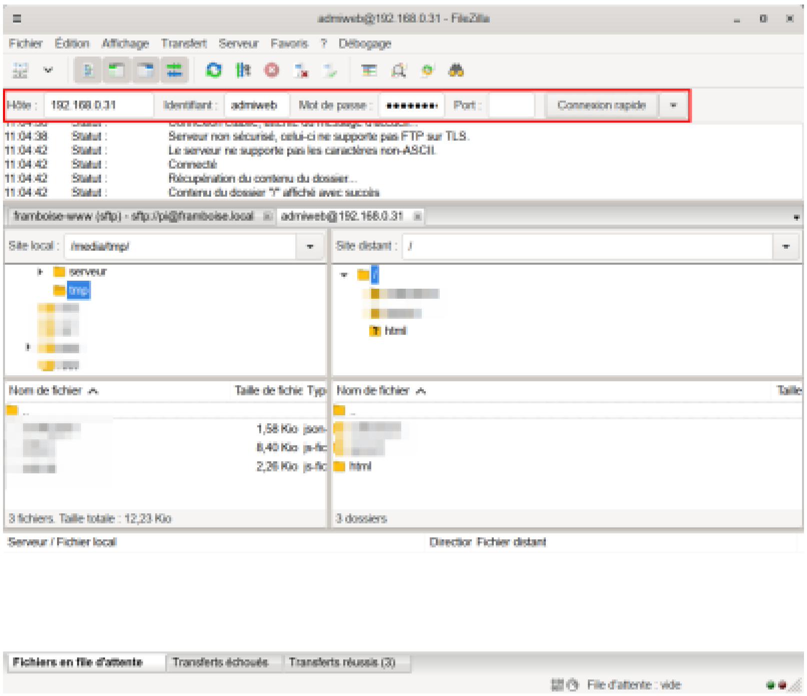
```
# Nom du serveur qui s'affiche
ServerName "ProFTPD Default Server"

# Serveur Autonome (ne pas modifier)
ServerType standalone

# Activer le serveur par défaut (Si pas de
"VirtualHost")
DefaultServer on

# Est-ce qu'on a besoin d'un shell valide pour
```

```
se connecter
RequireValidShell off

# Activer l'authentification PAM
AuthPAM off
AuthPAMConfig ftp

# Port d'écoute (21 par défaut)
Port 21

# Permissions d'un dossier ou d'un fichier créé
via FTP
Umask 022

# Nombre de connexions simultanées au FTP
MaxInstances 30

# Lancer le démon ftp sous cet utilisateur et
groupe
User ftp
Group ftp

# Racine du FTP ( [b]~[/b] correspond au fait
que l'utilisateur est cloisonné dans son dossier
personnel)
DefaultRoot ~

# Généralement, les fichiers peuvent être
écrasés.
AllowOverwrite on

# Désactiver la commande CHMOD via le FTP
<Limit SITE_CHMOD>
  DenyAll
</Limit>

# Exemple de dossier anonyme sans possibilité
d'uploader
<Anonymous ~ftp>
  User ftp
  Group ftp

  # Possibilité de se connecter avec les
utilisateurs "anonymous" et "ftp".
  UserAlias anonymous ftp

  # Limiter le nombre de connexions anonymes
  MaxClients 10

  # Désactiver la commande WRITE (d'écriture)
pour les utilisateurs anonymes
```

```
  <Limit WRITE>
    DenyAll
  </Limit>
</Anonymous>
```

Utilisation

Sur un PC du réseau, ouvrez Filezilla et lancez une connexion :



Hôte : 192.168.0.31 Identifiant : admiweb Mot de passe : •••••••• Port :

```
11:04:38    Statut :    Serveur non sécurisé, celui-ci ne supporte pas FTP sur TLS.
11:04:42    Statut :    Le serveur ne supporte pas les caractères non-ASCII.
11:04:42    Statut :    Connecté
11:04:42    Statut :    Récupération du contenu du dossier...
11:04:42    Statut :    Contenu du dossier "/" affiché avec succès
```

framboise-www (sftp) - sftp://pi@framboise.local | admiweb@192.168.0.31

Site local : /media/tmp/ Site distant : /

serveur
tmp
/
html

1,58 Kio json-
8,40 Kio js-fic
2,26 Kio js-fic

html

3 fichiers. Taille totale : 12,23 Kio

3 dossiers

- Hôte : l'adresse IP du serveur (ici, un Raspberry)
- Identifiant : admiweb
- Mot de passe : son mot de passe

Interface graphique : Gadmin-ProFTPd : une interface graphique pour le serveur FTP ProFTPd 🔧 Fix Me!

Désinstallation

Voir aussi

- **(fr)** http://arobaseinformatique.eklablog.com/mise-en-place-d-un-serveur-ftp-avec-proftpd-a105781016
- **(fr)** https://raspberrypi-tutorials.fr/comment-configurer-un-serveur-ftp-raspberry-pi-installation-du-serveur-web/

Basé sur « Comment configurer un serveur FTP Raspberry Pi – Installation du serveur Web » par raspberrypi-tutorials.fr.

From:
https://doc.nfrappe.fr/ - **Documentation du Dr Nicolas Frappé**

Permanent link:
https://doc.nfrappe.fr/doku.php?id=logiciel:internet:ftp:proftpd:start

Last update: **2022/11/08 19:28**