

# VsFTPd

## Généralités

- [VsFTPd](#)

## Installation

Installer le paquet de la distribution Cf. [Gestionnaire paquets GNU/Linux](#).

## Configuration générale

Emplacement	Fonction
/etc/vsftpd/vsftpd.conf	Cron exécuté tout les jours à 4h02 du matin.
/etc/vsftpd/ftpusers	Fichier avec la liste des utilisateurs qui n'ont pas le droit de se loguer en FTP.
/etc/vsftpd/chroot_list	Fichier avec la liste des utilisateurs qui doivent être chrootés.
/etc/vsftpd/user_list	Liste des Fichier avec la liste des utilisateurs qui n'ont pas le droit de se loguer en FTP.

## Configuration spécifique

Exemple avec deux comptes utilisateurs locaux standard nommés userlocal1 et userlocal2. Le compte userlocal1 doit pouvoir accéder au serveur FTP mais pas userlocal2.

Sauvegarde du fichier de configuration.

```
cd /etc/vsftpd
cp -p vsftpd.conf vsftpd.conf.orig
```

Changer les options suivantes avec les valeurs spécifiées.

```
ftpd_banner=Authorized access only.
anonymous_enable=NO #Desactivation des access anonymes
local_enable=YES #Autoriser les comptes locaux a se connecter
local_umask=002 #par défaut à 022. Pour permettre l'écriture des comptes
membres du même groupe
idle_session_timeout=3600 #Monter la valeur par default de desactivation de
session FTP
chroot_list_enable=YES #Activation d'une liste de compte chroote
chroot_list_file=/etc/vsftpd/chroot_list #Fichier de list de compte chroote
nopriv_user=ftp #Execution du service vsftpd avec un autre compte
utilisateur. Utilisation du compte ftp amene par le paquet client qui est en
/sbin/nologin.
userlist_enable=YES #Activation de la liste des utilisateurs interdit. Pas
```

```
de demande de password
dual_log_enable=YES #Activation de deux logs
log_ftp_protocol=YES #Activation du log FTP (connexion)
vsftpd_log_file=/var/log/vsftpd.log #selection du chemin du log des
connexions. Chemin par défaut pris en compte dans le logrotate par défaut.

xferlog_file=/var/log/xferlog #selection du chemin du log des transferts
FTP. Chemin par défaut pris en compte dans le logrotate par défaut.
pasv_enable=YES #activation mode passif
pasv_min_port=52000 #plage min des ports clients passif
pasv_max_port=54000 #plage max des ports clients passif
```

Création du fichier `/etc/vsftpd/chroot_list` avec la liste des comptes chrootés.

```
userlocal1
```

Ajout des comptes qui ne doivent pas pouvoir se connecter en FTP dans `/etc/vsftpd/ftpusers`. Avec uniquement cette liste, le mot de passe est quand même demandé. Erreur : login incorrect.

```
# Users that are not allowed to login via ftp
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
userlocal2
```

Ajout des comptes qui ne doivent jamais pouvoir se connecter en FTP dans `/etc/vsftpd/user_list`. Un utilisateur dans cette liste sera automatiquement interdit. La demande de mot de passe n'est pas demandé.

```
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
```

```
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
userlocal2
```

Démarrer le service.

```
/etc/init.d/vsftpd start
```

L'ajouter au démarrage du système.

```
chkconfig --list vsftpd
chkconfig vsftpd on
```

## Exemple fichier configuration

```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this
# out).
#anonymous_enable=YES
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you
```

```
will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
dual_log_enable=YES
# The target log file can be vsftpd_log_file or xferlog_file.
# This depends on setting xferlog_std_format parameter
xferlog_enable=YES
#
log_ftp_protocol=YES
vsftpd_log_file=/var/log/vsftpd.log
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# The name of log file when xferlog_enable=YES and xferlog_std_format=YES
# WARNING - changing this filename affects /etc/logrotate.d/vsftpd.log
#xferlog_file=/var/log/xferlog
#
# Switches between logging into vsftpd_log_file and xferlog_file files.
# NO writes to vsftpd_log_file, YES to xferlog_file
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
idle_session_timeout=3600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
nopriv_user=ftp
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
```

```
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do
ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner>Welcome to blah FTP service.
ftpd_banner=Bienvenue sur le serveur FTP du Sifec.
#
# You may specify a file of disallowed anonymous e-mail addresses.
Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror"
assume
# the presence of the "-R" option, so there is a strong case for enabling
it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and
IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES
```

```
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

## Fichiers de logs

- /var/log/xferlog : log des transactions.
- /var/log/vsftpd.log : log des connexions.

## Rotation des logs

Tester la connexion avec les comptes utilisateurs.

Modification de la rotation des logs pour éviter de saturer le filesystem /var. Conservation des 4 derniers jours et compression des logs.

```
/etc/logrotate.d/vsftpd
```

```
/var/log/vsftpd.log {
    # ftpd doesn't handle SIGHUP properly
    daily
    compress
    missingok
}

/var/log/xferlog {
    # ftpd doesn't handle SIGHUP properly
    daily
    compress
    missingok
}
```

## Test FTP

- Cf. [Test FTP](#).

From:  
<https://wiki.ouieuhtoutca.eu/> - **kilsufi de noter**

Permanent link:  
<https://wiki.ouieuhtoutca.eu/vsftpd>

Last update: **2021/01/21 21:42**

