

Logiciel

VSFTPD : un serveur FTP sécurisé avec des utilisateurs virtuels

vsftpd est un serveur FTP stable, sécurisé et rapide.

Nous allons l'installer et le configurer ainsi :

- Seuls les utilisateurs locaux sont autorisés à se connecter au serveur
- En lecture seule
- Les utilisateurs ne peuvent pas accéder à leurs répertoires
- Les options seront réglées utilisateur par utilisateur
- les utilisateurs seront restreints à leur répertoire d'origine
- les transmissions seront cryptées avec un certificat auto-signé SSLTLS.
- nous utiliserons le paramétrage par **utilisateurs virtuels**, avec une base de données de type **Berkeley**.

Chaque enregistrement n'est constitué que d'un login et d'un mot de passe.

Pour créer un nouvel utilisateur, il suffit de lui créer :

- une entrée dans la base Berkeley
- et un fichier de configuration personnel.

Quatre scénarios illustreront les possibilités.



Le protocole ftp en lui même n'est pas sûr !

L'échange du nom d'utilisateur et du mot de passe transite en clair sur le réseau.

N'utilisez pas via ftp un compte qui a les droits sudo !



Nous supposons que le serveur sera sur le disque
`$DISQUE=/srv/www`

Pré-requis

Installation

Mettez à jour :

```
...@...:~$ sudo apt update
```

Installez les paquets :

```
...@...:~$ sudo apt install vsftpd db-util ftp
```

Le service ftp démarre automatiquement après l'installation.

Vérifiez avec le programme **ftp** :

- Acceptez le nom d'utilisateur proposé et donnez son mot de passe (par exemple, sur un Raspberry pi : **pi** / **raspberrypi**).
- Pour sortir du ftp : **bye**
- Avec la configuration d'origine, le serveur fonctionne :
 - avec un utilisateur (**pi**) disposant réellement d'un compte sur la machine serveur
 - mais **pas en anonyme** (impossible de se connecter avec l'utilisateur *anonymous*)
 - un ls confirme que le dossier racine est le home (**/home/pi**) de cet utilisateur

```
...@...:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.3)
Name (localhost:pi):
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
...
drwxr-xr-x    8 1000    1000          4096 Aug 01 21:59
Documents
...
226 Directory send OK.
ftp> bye
221 Goodbye.
...@...:~$
```

4. depuis un PC du réseau, en vous connectant avec un logiciel comme FileZilla, avec un user/password de la machine

- vous pouvez :
 - vous déplacer dans toute la machine serveur, y compris la racine
 - télécharger un fichier depuis le serveur

2. mais pas :

- y écrire ou téléverser un fichier
- ni créer un répertoire
- ni effacer un fichier ou un répertoire

- L'installation de vsftpd a créé l'utilisateur **ftp**, dont le home est **/srv/ftp** et le groupe **ftp**:

```
...@...:~$ cat /etc/passwd |  
grep ftp  
ftp:x:117:124:ftp  
daemon,,,:/srv/ftp:/usr/sbin/nol  
ogin
```

- Si ce n'est pas le cas, créez-les :

```
...@...:~$ sudo groupadd ftp
```

- Si l'utilisateur ftp existe, vous pouvez lui donner comme home le répertoire de base du serveur ftp :

```
...@...:~$ sudo usermod -d  
<disque>/ftp ftp
```



2. Et l'installation d'un serveur HTTP crée l'utilisateur **www-data**, dont le home est **/var/www**:

```
...@...:~$ cat /etc/passwd |  
grep www-data  
www-data:x:33:33:www-  
data:/var/www:/usr/sbin/nologin
```

Configuration

Le fichier de configuration du serveur est **/etc/vsftpd.conf** : **Le fichier de configuration de vsftpd**. Voir la page de man **Page de man vsftpd.conf**



Explication des options :

Créez le répertoire **/etc/vsftpd/user_conf**
et le fichier **/etc/vsftpd/user_list**:

```
...@...:~$ sudo mkdir -p  
/etc/vsftpd/user_conf  
...@...:~$ sudo touch  
/etc/vsftpd/user_list
```

Sauvegardez les fichiers de configuration originaux :

```
...@...:~$ sudo cp  
/etc/vsftpd.conf  
/etc/vsftpd.conf.dist  
...@...:~$ sudo cp  
/etc/pam.d/vsftpd  
/etc/pam.d/vsftpd.dist
```



Pour revenir au départ en cas de problème,
il suffira de faire l'inverse :

```
...@...:~$ sudo cp  
/etc/vsftpd.conf.dist  
/etc/vsftpd.conf  
...@...:~$ sudo cp  
/etc/pam.d/vsftpd.dist  
/etc/pam.d/vsftpd
```

créez un **emplacement pour la racine du serveur** :

- Créez le répertoire
<DISQUE>/srv/ftp :

```
...@...:~$ sudo mkdir -p  
<DISQUE>/srv/ftp
```

- Éditez avec les droits d'administration
le fichier **/etc/fstab** pour ajouter la
ligne :

[/etc/fstab](#)

```
<DISQUE>/srv /srv
```

```
none    bind    0
0
```

- Montez **/srv** :

```
...@...:~$ sudo mount /srv
```

Configuration par défaut

Éditez avec les droits d'administration le fichier **/etc/vsftpd.conf** pour ajouter à la fin les commandes suivantes.

Commandes

Nous plaçons à la fin du fichier **/etc/vsftpd.conf** nos réglages par défaut :

Paramètres généraux :



[/etc/vsftpd.conf](#)

```
...
##### Paramètres
personnalisés
#####
ftpd_banner=Bienvenue
sur le serveur FTP de
...

# un message apparaît
chaque fois
# qu'un utilisateur
ouvre un répertoire
avec un fichier
.message
dirmessage_enable=YES

# heure locale de
l'ordinateur au lieu de
l'heure GMT
use_localtime=YES

# Nombre maximum de
connexions simultanées
#   Au-delà, les
```

```
nouveaux clients
recevront un message du
genre :
# "erreur: serveur
occupé"
max_clients=200
# Nombre maximum de
connexions venant de la
même IP
max_per_ip=4

# journalisation des
transferts
xferlog_enable=YES
```

Utilisateurs virtuels :

[/etc/vsftpd.conf](#)



```
# Activation des
utilisateurs virtuels
guest_enable=YES
# nom de l'utilisateur
(ftp) sous lequel ils
vont fonctionner
# tous les
utilisateurs virtuels
-> utilisateur ftp avec
son home /srv/ftp
ftp_username=ftp
guest_username=ftp
nopriv_user=ftp

# Fichier de config PAM
pam_service_name=vsftpd
```

Connexion et contrôle d'accès :

[/etc/vsftpd.conf](#)

```
# Pas d'accès anonyme,
que des utilisateurs
locaux
# (dont les
utilisateurs virtuels,
mappés sur un
utilisateur local)
# les vrais
utilisateurs locaux
sont désactivés avec le
```

```
fichier user_list
anonymous_enable=NO
local_enable=YES

# On refuse les
utilisateurs du fichier
/etc/vsftpd.user_list
# un utilisateur par
ligne
userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/vsft
pd/user_list

# Les utilisateurs
locaux restent chez eux
chroot_local_user=YES
allow_writeable_chroot=
YES
```

Permissions :

[/etc/vsftpd.conf](#)



```
# Interdiction de toute
action d'écriture :
# On spécifiera les
droits utilisateur par
utilisateur.
write_enable=NO
anon_mkdir_write_enable
=NO
anon_other_write_enable
=NO
anon_upload_enable=NO
anon_world_readable_onl
y=NO

# droits par défaut des
fichiers uploadés
anon_umask=002

# Autoriser les
utilisateurs locaux
# à changer les
permissions des
fichiers
chmod_enable=YES
virtual_use_local_privs
=YES
```

```
# On n'autorise pas les
utilisateurs à se faire
passer pour d'autres
chown_uploads=NO
chown_username=nobody

# Cacher les
informations sur le
propriétaire des
fichiers (utilisateur
et groupe)
hide_ids=YES

# Activation de la
configuration
utilisateur par
utilisateur
user_config_dir=/etc/vs
ftpd/user_conf
```

Sécurisation des transmissions avec SSL/TLS :

[/etc/vsftpd.conf](#)



```
rsa_cert_file=/etc/ssl/
private/vsftpd.pem
rsa_private_key_file=/e
tc/ssl/private/vsftpd.p
em
ssl_enable=YES
```

après avoir créé la clé privée de 2048 bits et le certificat autosigné valable 10 ans (la clé privée et le certificat sont enregistrés dans un même fichier) :

```
...@...:~$ sudo openssl req -
x509 -nodes -days 3650 -newkey
rsa:2048 -keyout
/etc/ssl/private/vsftpd.pem -out
/etc/ssl/private/vsftpd.pem
```

Utilisateurs virtuels



Nous allons créer trois utilisateurs virtuels :



admin, qui aura accès à tout **/srv** sous l'utilisateur **ftp**

user, qui ne pourra que télécharger sous l'utilisateur **ftp**

admiweb, qui aura accès à tout le site web (**/serv/www/html**) sous l'utilisateur **www-data**

Éditez avec les droits d'administration le fichier `/etc/vsftpd/login.txt` pour y écrire les noms et mots de passe des utilisateurs virtuels (2 lignes pour chaque utilisateur) :

[/etc/vsftpd/login.txt](#)



```
admin
MotDePasseAdmin
user
MotDePasseUser
admiweb
MotDePasseAdmiweb
```

N'oubliez pas une ligne vide à la fin.

Créez la base de données :

```
...@...:~$ sudo db_load -T -t
hash -f /etc/vsftpd/login.txt
/etc/vsftpd/login.db
```

Protégez ces fichiers contre une intrusion :

```
...@...:~$ sudo chmod 600
/etc/vsftpd/login.*
```



Pour ajouter, modifier ou supprimer un utilisateur il faut éditer le fichier `login.txt` puis relancer la création de la base avec



la commande du
paragraphe 2.

**Éditez avec les droits d'administration
le fichier `/etc/pam.d/vsftpd` et remplacez
son contenu par :**

`/etc/pam.d/vsftpd`

```
auth required
pam_userdb.so
db=/etc/vsftpd/login
account required
pam_userdb.so
db=/etc/vsftpd/login
```

Redémarrez le serveur :

```
...@...:~$ sudo systemctl
restart vsftpd.service
```



Vérification :

- pi ne peut plus se connecter :

```
...@...:~$ ftp localhost
Connected to localhost.
220 Bienvenue sur le serveur
FTP de xxx
Name (localhost:pi):
331 Please specify the
password.
Password:
530 Login incorrect.
Login failed.
ftp> bye
221 Goodbye.
```

- mais admiweb le peut :

```
ftp localhost
Connected to localhost.
220 Bienvenue sur le serveur
FTP de xxx
Name (localhost:pi): admiweb
331 Please specify the
password.
Password:
```

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to
transfer files.
ftp> bye
221 Goodbye.
```

Deux scripts pour se faciliter la vie

txt2db.sh régénère le fichier .db et crée un fichier de config vide s'il n'existe pas (le script est supposé résider en **~/bin/**) :

`~/bin/txt2db.sh`



```
#!/bin/sh
if [ $# =
"2" ];
then
    rm -f
    $2
    db_load -
    T -t hash
    -f
    /etc/vsft
    pd/$1
    /etc/vsft
    pd/$2
    chmod
    600
    /etc/vsft
    pd/login.
    *
    echo
    "Base
    créée"
    lignes=$(
    cat $1)
    nb=1
    for
    ligne in
    $lignes
    do
    if [
```



```
$(($nb%2)
) -ne 0
];
then
if [ ! -e
/etc/vsft
pd/user_c
onf/$lign
e ];
then
touch
/etc/vsft
pd/user_c
onf/$lign
e
echo
"fichier
/etc/vsft
pd/user_c
onf/$lign
e créé"
fi
fi
nb=$(($nb
+1))
done
else
echo
"Il faut
donner le
fichier
d'entrée
et le
fichier
de
sortie"
fi
```

Rendez-le exécutable (à ne faire que la première fois) :

```
...@...:~$ sudo
chmod +x
~/bin/txt2db.sh
```

Utilisation (le script est supposé résider en **~/bin/**) :

```
...@...:~$ cd ~/bin
...@...:~$ sudo
./txt2db.sh
login.txt login.db
```

Ce script lit les lignes du login.txt ; pour chaque login, il vérifie si un fichier de configuration existe. Si ce n'est pas le cas il en crée un vide.

Auparavant il génère le fichier db.

Le script **cleanconf.sh** supprime tous les fichiers qui n'ont pas de login associé (utilisateurs supprimés) :

`~/bin/cleanconf.sh`



```
fichiers=
$(ls
/etc/vsft
pd/user_c
onf)
users=""
lignes=$(
cat
/etc/vsft
pd/login.
txt)
nb=1
for ligne
in
$lignes
do
    if [
$(( $nb%2
) -ne 0
];
    then
users="$u
sers
$ligne"
    fi
nb=$(( $nb
+1))
done
```



```
for conf
in
$fichiers
do
found=0
    for
user in
$users
    do
if [
$conf =
$user ];
then
found="1"
fi
    done
    if [
$found !=
"1" ];
then
rm -f
/etc/vsft
pd/user_c
onf/$conf
echo
"Fichier
/etc/vsft
pd/user_c
onf/$conf
supprimé"
fi
done
```

Rendez-le exécutable (à ne faire que la première fois) :

```
...@...:~$ sudo
chmod +x
~/bin/cleanconf.sh
```

Utilisation (le script est supposé résider en **~/bin/**) :

```
...@...:~$ cd ~/bin
...@...:~$ sudo
./cleanconf.sh
```

Personnalisation pour chaque utilisateur

Par défaut les utilisateurs virtuels n'ont aucun droit.

Il faut donc les définir pour chacun d'entre eux en créant dans le dossier **/etc/vsftpd/user_conf** un fichier de configuration pour chaque utilisateur (du même nom que le login de l'utilisateur auquel il fait référence).

Chaque fichier contient des paramètres (les mêmes que ceux de vsftpd.conf) qui remplaceront ceux de vsftpd.conf.

Généralement, on y modifie le "local_root" et les droits d'écriture.

Voici quelques exemples.

utilisateur **admin** :



[/etc/vsftpd/user_conf/admin](#)

```
# Racine
local_root=/srv

# Lecture autorisée
download_enable=YES
anon_world_readable_only=NO

# Écriture autorisée
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES

# Renommage et suppression autorisés
anon_other_write_enable=YES

# changement des droits autorisé
chmod_enable=YES
virtual_use_local_privs=YES
```

```
# Définit à qui
appartiendront les
fichiers téléversés
guest_username=pi

# Affichage des
fichiers cachés
#   (important pour les
fichiers htaccess)
force_dot_files=YES

# masque local (002 ->
droits 775)
local_umask=002
anon_umask=002
```

Cet utilisateur aura presque tous les droits et accédera au répertoire /srv et à tous ses sous-répertoires.

utilisateur **admiweb** :

/etc/vsftpd/user_conf/admiweb



```
# Racine
local_root=/srv/www/html

# Lecture autorisée
download_enable=YES
anon_world_readable_only=NO

# Écriture (upload)
autorisée
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES

# Renommage et
suppression autorisés
anon_other_write_enable=YES

# changement des droits
autorisé
chmod_enable=YES
virtual_use_local_privs=YES
```



```
# Définit à qui
appartiendront les
fichiers téléversés
guest_username=www-data
chown_uploads=YES
chown_username=www-data

# Affichage des
fichiers cachés
# (important pour les
fichiers htaccess)
force_dot_files=YES

# masque local (002 ->
droits 775)
file_open_mode=0777
local_umask=002
anon_umask=002
```

Cet utilisateur aura presque tous les droits et accédera au répertoire **/srv/www/html** et à tous ses sous-répertoires sous le nom **www-data**



utilisateur **user** :

- Créez le répertoire
<DISQUE>/srv/ftp/user :

```
...@...:~$ sudo mkdir -p
<DISQUE>/srv/ftp/user
```

- puis le fichier

/etc/vsftpd/user_conf/user

```
local_root=/srv/ft
p/user
```

Cet utilisateur ne pourra que télécharger et sera enfermé dans le répertoire **/srv/ftp/user** (qui doit exister).

4. utilisateur **adminftp** :

/etc/vsftpd/vsftpd_user_conf/adminftp

```
## l'utilisateur est
```



```
enfermé dans un dossier
déterminé
# en commentant cette
ligne, on autorise tout
le site
#local_root=adminftp

## droit de
lecture(download)
anon_world_readable_onl
y=NO

## droit
d'écriture(upload)
write_enable=YES
anon_upload_enable=YES

## créer des dossiers
anon_mkdir_write_enable
=YES

## droit de renommer,
supprimer...
anon_other_write_enable
=YES

## pour gérer le chmod
de l'utilisateur
## activer l'option
#virtual_use_local_priv
s=YES
## définir l'option
local_umask
#local_umask=022
#anon_umask=022
write_enable=YES
anon_upload_enable=YES
```

adminftp aura accès au répertoire ~ftp et à ses sous-répertoires avec tous les droits ; il ne pourra pas remonter au-dessus de ~ftp qui apparaîtra comme la racine "/"

Redémarrez le serveur pour valider les modifications :

```
...@...:~$ sudo systemctl
restart vsftpd.service
```

Tests

admin :

```
...@...:~$ ftp localhost
Connected to localhost.
220 Bienvenue sur le serveur FTP
de framboise 4.
Name (localhost:pi): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer
files.
ftp> bye
221 Goodbye.
```

- connexion possible
- peut lister le répertoire, écrire, ajouter ou effacer ce qu'il veut
- à partir de la racine **/srv**

2. admiweb :



```
...@...:~$ ftp localhost
Connected to localhost.
220 Bienvenue sur le serveur FTP
de framboise 4.
Name (localhost:pi): admiweb
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer
files.
ftp> bye
221 Goodbye.
```

- connexion possible
- peut lister le répertoire, écrire, ajouter ou effacer ce qu'il veut
- à partir de la racine **/srv/www/html**
- les fichiers téléversés appartiennent à **www-data**

3. user :

```
...@...:~$ ftp localhost
```

```
Connected to localhost.
220 Bienvenue sur le serveur FTP
de framboise 4.
Name (localhost:pi): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer
files.
ftp> bye
221 Goodbye.
```

- connexion possible
- ne peut que télécharger
- à partir de **/srv/www** seulement

4. connexion **impossible** pour :

- un **utilisateur réel** de la machine (pi)
:

```
...@...:~$ ftp localhost
...
Name (localhost:pi):
331 Please specify the
password.
Password:
530 Login incorrect.
Login failed.
ftp> bye
221 Goodbye.
```

- ni en **anonyme**

Cinq exemples de configuration

Voir la page [Vsftpd : cinq exemples de configuration](#)

Utilisation

Gestion du service

Via systemctl :



```
...@...:~$ sudo systemctl  
COMMANDE vsftpd
```

Valeurs de COMMANDE :

start	Démarrer le serveur
stop	Arrêter le serveur
restart	Redémarrer le serveur
status	État du serveur

Se connecter en utilisant le serveur FTP comme un simple dossier

Sous Ubuntu

- Raccourcis (menu en haut)
- Se connecter à un serveur



- **type de service** : ftp (avec identification)
- **l'adresse du serveur** :
- **le nom d'utilisateur**
- et Se connecter

On peut aussi cocher la case pour créer un signet en le nommant.

On se retrouve avec un dossier distant dans lequel on peut naviguer.

Ne pas oublier de se déconnecter (démonter)

Sous Windows

- Double-clic sur Favoris réseau
- puis sur Ajouter un favori réseau
- cliquer sur Suivant deux fois de suite
- saisir, dans le champ Adresse réseau ou Internet, la ligne
<ftp://identifiant:motdepasse@adresse devotresiteftp/>
- Suivant
- taper l'adresse du site dans le champ Entrez un nom pour ce favori réseau
- Suivant
- Terminer.

Désormais, on peut se connecter directement sur le serveur FTP, en :

- double-cliquant sur Favoris réseau
- puis sur l'icône du serveur
- et ainsi accéder aux dossiers et fichiers qu'il contient dans la limite des droits accordés.



Désinstallation

Désinstallation partielle : Pour désinstaller le serveur vsftpd, en gardant les fichiers de configuration :

```
$ sudo apt-get remove vsftpd
```

Pour tout remettre à plat :

```
...@...:~$ sudo apt remove --  
purge vsftpd db-util  
...@...:~$ sudo mv  
/etc/vsftpd.conf.dist  
/etc/vsftpd.conf  
...@...:~$ sudo mv  
/etc/pam.d/vsftpd.dist  
/etc/pam.d/vsftpd
```



La remise à plat supprime définitivement des

données de votre disque dur !



Si vous n'êtes pas sûr de vous, la désinstallation partielle est préférable.

Voir aussi

- **(fr)** <https://linuxize.com/post/how-to-setup-ftp-server-with-vsftpd-on-raspberry-pi/>

VSFTPD

- Documentation spécifique dans le répertoire **/usr/share/doc/vsftpd/** et les **man**
- **(fr)** <http://linux.developpez.com/vsftpd/#L2.2>
- **(fr)** [https://debian-facile.org/utilisateurs:hyathie:tutos:vsftpd?s\[\]=vsftpd](https://debian-facile.org/utilisateurs:hyathie:tutos:vsftpd?s[]=vsftpd)
- **(fr)** Doc Ubuntu sur VSFTPD
- **(fr)** <http://www.loutre.ch/installer-un-serveur-ftp-chroote-avec-vsftpd-en-5-minutes>
- **(fr)** <http://www.commentcamarche.net/faq/3028-installer-un-serveur-ftp-sous-windows>
- **(en)** Page officielle du projet
- **(en)** Page consacrée à vsFTPd sur freshmeat : <http://freshmeat.net/projects/vsftpd/>



2. vsftpd.conf

- **(en)** Page de manuel : http://vsftpd.beasts.org/vsftpd_conf.html
- **(fr)** principales options de vsftpd.conf : <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-fr-4/s1-ftp-vsftpd-conf.html>
- **(fr)** Toutes les directives traduites en français :

<http://www.walkonthegrass.net/tutoriels/Linux/vsftpd>

3. VSFTPD sur un Raspberry Pi

- **(en)** [How to Setup FTP Server with Vsftpd on Raspberry Pi](#)
- **(fr)** [Spécification du protocole FTP](#)
- **(en)** <https://security.appspot.com/vsftpd.html>

Utilisateurs virtuels

- **(fr)** [Page de manuel de PAM](#)
- **(fr)** Les pages de supinfo : <http://www.labo-linux.com/articles/imported/3259-vsftpd-et-utilisateurs-virtuels>
- **(en)** Pour gérer votre db Berkeley : <http://www.sleepycat.com/docs/utility/index.html>
- **(fr)** un mémo, complété d'après la doc : http://doc.ubuntu-fr.org/vsftpd#configurer_vsftpd_pour_utiliser_des_utilisateurs_virtuels
- **(fr)** configuration d'un ftp avec utilisateurs virtuels : <http://www.prometee-creation.com/tutoriels/un-serveur-ftp-avec-vsftpd-et-utilisateurs-virtuels.html>



2. Didacticiels

- **(fr)** [Un tuto excellent avec quatre exemples](#)
- **(en)** <ftp://vsftpd.beasts.org/users/cevans/untar/vsftpd-2.0.3/EXAMPLE/>

3. FAQ :

- **(en)** <ftp://vsftpd.beasts.org/users/cevans/untar/vsftpd-2.0.3/FAQ>
- **(fr)** [vsftpd FAQ \(traduction de questions fréquemment posées\)](#)

Basé sur « [Article](#) » par Auteur.



From:
<https://nfrappe.fr/doc-0/> - **Documentation du Dr Nicolas Frappé**

Permanent link:
<https://nfrappe.fr/doc-0/doku.php?id=logiciel:internet:ftp:vsftpd:start> 

Last update: **2022/08/13 22:14**