

Installation et configuration d'un serveur FTP

Ressources :

- https://doc.ubuntu-fr.org/vsftpd_et_pam_mysql
- <http://www.debianaddict.org/article47.html>
- <http://docs.btssio.ac-limoges.fr/docs/doku.php?id=administration:valadon:esxprof:hebergementweb>

Présentation

Le serveur FTP doit permettre d'**héberger les dossiers** de **différents utilisateurs**. Cependant ce sont des **comptes virtuels**, gérés dans une base de données **MySQL**, qui seront utilisés afin d'éviter de créer des comptes linux sur le serveur.

Préparation du serveur

Le serveur doit disposer du serveur Web Apache2, de PHP, MySQL et PhpMyAdmin.

Mise à jour du serveur

```
# apt-get update  
# apt-get upgrade
```

Configuration de MySQL

Création d'un compte et d'une base de données pour ftp

- création avec **phpmyadmin** d'un compte **ftp** local avec sa base de données **ftp** sur laquelle il a tous les privilèges.

Installation et configuration de vsFTPD pour l'hébergement multi-utilisateur

Installer vsFTPD

```
apt install vsftpd
```

Il faut supprimer l'utilisateur **ftp** créé par défaut :

```
# deluser --remove-home ftp
```

Modifiez le fichier de configuration **/etc/vsftpd.conf** pour :

- utilisation en mode standalone
- désactiver les connexion anonymes
- activer les connexions des utilisateurs locaux
- interdire toutes actions d'écriture
- interdire l'upload anonyme
- interdire la création de répertoire anonyme
- définir des droits par défaut des fichiers uploadés (droits en 755)
- activer les utilisateurs virtuels et les faire correspondre à www-data
- enfermer les utilisateurs virtuels dans leur dossier
- définir le nombre maximum de session à 100 et le nombre maximum de session par IP à 5
- Définir la plage de ports utilisés par le mode passif de 20000 à 20050
- Définir la plage de ports utilisés par le mode passif
- Autoriser les utilisateurs virtuels à changer les permissions de leurs fichiers
- Activer les logs
- Définir valeur de timeout
- Interdire la commande ABOR pas sécurité
- S'assurer que la commande PORT provient bien du port 20 du client
- Utilisation des configurations individuelles pour chaque utilisateur

- Définir les heures d'enregistrement à l'heure locale
- définir la bannière d'accueil

Les lignes concernées :

```
# utilisation en mode standalone
listen=YES
# désactiver les connexion anonymes
anonymous_enable=NO
# activer les connexions des utilisateurs locaux
local_enable=YES
# interdire toutes actions d'écriture
write_enable=NO
# interdire l'upload anonyme
anon_upload_enable=NO
# interdire la création de répertoire anonyme
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
allow_anon_ssl=NO
# définition des droits par défaut des fichiers uploadés (droits en 755)
local_umask=022
# activer les utilisateurs virtuels
guest_enable=YES
# faire correspondre tous les utilisateurs virtuels à l'utilisateur d'Apache 2 (www-data)
guest_username=www-data
# Enfermer les utilisateurs virtuels dans leur dossier
chroot_local_user=YES
chroot_list_enable=NO
# Dossier utiliser pour le chroot (doit appartenir à root et avec un chmod 755)
# car il ne doit surtout pas être inscriptible (writable) par tous le monde
secure_chroot_dir=/var/run/vsftpd/empty

# définir le nombre maximum de session à 100
max_clients=100
# définir le nombre maximum de session par IP à 5
max_per_ip=5
# Définir la plage de ports utilisés par le mode passif
pasv_min_port=20000
pasv_max_port=20050

# Autoriser les utilisateurs virtuels à changer les permissions de leurs fichiers
chmod_enable=YES
virtual_use_local_privs=YES

# Activer les logs
xferlog_enable=YES
log_ftp_protocol=YES
xferlog_file=/var/log/vsftpd.log
# Définir valeur de timeout
idle_session_timeout=300
data_connection_timeout=120
connect_timeout=60
accept_timeout=60
# Interdire la commande ABOR pas sécurité
async_abor_enable=NO
# S'assurer que la commande PORT provient bien du port 20 du client
connect_from_port_20=YES

# Utilisation des configurations individuelles pour chaque utilisateurs
user_config_dir=/etc/vsftpd
# Définir les heures d'enregistrement à l'heure locale
use_localtime=YES
# définir la bannière
ftpd_banner=Serveur FTP de test - Charles Técher.
# enlever la mesure de sécurité de vsftpd qui empêche un client de chrooter un client dans un répertoire
# pour il possède les droits d'écriture.
# https://lindex.fr/index.php?post/2013/04/05/wheezy-vsftpd-et-chroot
allow_writeable_chroot=YES
```

Gestion des autorisations sur le dossier `securechrootdir (/var/run/vsftpd/empty)` avec les permissions adéquates : il ne faut pas que les

utilisateurs aient des droits d'écriture dans ce répertoire.

```
$ chown root:root /var/run/vsftpd/empty
$ chmod 660 /var/run/vsftpd/empty
```

Création du dossier contenant les configurations de chaque utilisateur :

```
mkdir /etc/vsftpd
```

Configurer vsFTPD avec pam-mysql

Il faut installer le module d'authentification par MySQL !

```
# apt-get install libpam-mysql
```

Création de la table des utilisateurs dans la base de données ftp.

- lancer **PHPMysqlAdmin**,
- se logger avec l'utilisateur **ftp** et sélectionner la base de donnée **ftp**,
- créer la table **ftp** ci-dessous :

```
CREATE TABLE `ftp`.`users` (
  `name` TEXT NOT NULL ,
  `pass` TEXT NOT NULL
) ENGINE = MYISAM
```

Remplacer le contenu du fichier **/etc/pam.d/vsftpd** par le suivant (qui contient les informations d'accès à cette table) :

```
auth required pam_mysql.so host=localhost user=ftp passwd=votre_pass db=ftp table=users usercolumn=name
passwdcolumn=pass crypt=1
account required pam_mysql.so host=localhost user=ftp passwd=votre_pass db=ftp table=users
usercolumn=name passwdcolumn=pass crypt=1
```

Redémarrer le serveur FTP !

```
/etc/init.d/vsftpd restart
```

Principe de la création d'un site

- Définir un **nom de compte** et un **mot de passe** ;
- connexion à la base de données **ftp** avec le compte et le mot de passe de l'utilisateur **ftp**,
- Dans la base de données ftp, il faut ajouter un nouvel enregistrement à la table en renseignant avec le nom d'utilisateur et le mot de passe crypté avec l'option ENCRYPT.
- création du fichier de configuration de l'utilisateur **/etc/vsftpd/[nom d'utilisateur]**.

```
anon_world_readable_only=NO
local_root=/home/[nom d'utilisateur]/public_html
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES
anon_other_write_enable=YES
hide_file=(none)
force_dot_files=YES
```

Pour davantage d'informations sur les options choisies, voir la page de documentation http://vsftpd.beasts.org/vsftpd_conf.html. (définition du dossier dans lequel l'utilisateur est enfermé, on l'autorise à y écrire, et on lui permet de voir les fichiers cachés).

- création du dossier de l'utilisateur avec les bons droits : `mkdir /home/[nom d'utilisateur] chown -R www-data:www-data /home/[nom d'utilisateur] chmod -R 700 /home/[nom d'utilisateur]`
- L'utilisateur accède par ftp à son dossier à l'adresse <ftp://spock.btssio.local> avec le [nom d'utilisateur] et son mot de passe.
- On accède au site web à l'adresse [http://spock.btssio.local/~\[nom d'utilisateur\]](http://spock.btssio.local/~[nom d'utilisateur])

From:

/ - **Les cours du BTS SIO**

Permanent link:

</doku.php/reseau/debian/ftp/accueil>

Last update: **2019/01/30 12:58**

