Centos: Mise en oeuvre d'un serveur FTP avec VsFTPd

Table of Contents

Cet article décrit la mise en place d'un serveur FTP avec VsFTPd (Very Secure FTP Daemon) sur un serveur de réseau local tournant sous CentOS. FTP est la manière la plus simple pour échanger des fichiers sur le réseau.

Présentation

VsFTPd est un serveur FTP conçu avec la problématique d'une sécurité maximale. Contrairement aux autres serveurs FTP (ProFTPd, PureFTPd, etc.), aucune faille majeure de sécurité n'a jamais été décelée dans VsFTPd.

Vsftpd et Sftp

Il est important de ne pas confondre cette évolution sécurisée de FTP, basée sur le protocole d'origine, avec SFTP.

SFTP n'est nullement basé sur FTP, mais sur SSH. Il fait d'ailleurs partie de OpenSSH server et n'utilise par défaut que l'unique port 22 de SSH.

SFTP peut être vu comme un SCP avec une interface de commande proche de FTP, les mêmes possibilités d'utilisation sur un lien peu fiable (une copie avortée par une perte de connexion ne devra pas être reprise de zéro, mais reprendra de là ou elle en était une fois le lien ré-établi)... D'ailleurs la plupart des clients FTP classiques supportent SFTP (parfois dénommé FTP sous SSH2).

FTP actif et FTP passif

Avant de démarrer une petite explication sur les deux modes de transfert de fichiers FTP.

Le mode FTP actif

Est le mode par défaut des clients FTP. Dans un premier temps, une session TCP est initiée sur le port 21 du serveur. Une fois la session établie et l'authentification FTP acceptée, le serveur établit une session TCP depuis le port 20 vers un port dynamique du client.

Le mode FTP passif

Est conseillé à partir du moment où les clients peuvent se trouver derrière un pare-feu. Dans ce mode, toutes les initialisations de sessions TCP se font à partir du client. Là aussi, le client établit une première session TCP sur le port 21. La session est établie, l'authentification est acceptée, et à partir de là, on demande au serveur de se mettre en attente de session TCP grâce à la commande PASV. Le client peut alors établir une seconde session TCP sur un port dynamique vers le serveur.

Le numéro de port dynamique est transmis du serveur vers le client suite à la commande PASV. On peut réduire la plage de ports en configurant le serveur FTP de manière appropriée, et c'est ce que nous allons faire ici. Configuration du pare-feu

Du côté pare-feu une configuration un peu particulière avec le protocole FTP est nécessaire pour permettre l'accès au serveur, il faut:

- charger le module ip*conntrack*ftp
- ouvrir le port 21 en TCP
- ouvrir les ports 50001 à 50010 en TCP pour le mode passif

Voici à quoi cela ressemble concrètement dans un script de pare-feu.

```
...
IPT=/usr/sbin/iptables
```

```
MOD=/usr/sbin/modprobe
...
# FTP
$MOD ip_conntrack_ftp
$IPT -A INPUT -p tcp -i $IFACE_LAN --dport 21 -j ACCEPT
$IPT -A INPUT -p tcp -i $IFACE_LAN --dport 50001:50010 -j ACCEPT
...
```

Configuration de SELinux: Lorsqu'on utilise **SELinux** en mode renforcé sur le serveur, il suffit de modifier la valeur par défaut du booléen **ftpd_full_access** comme ceci:

```
setsebool -P ftpd_full_access 1
```

À partir de là, **SELinux** ne posera aucun problème.

Installation et configuration du serveur

Installer le serveur

Le serveur VsFTPd est fourni par les dépôts officiels de Red Hat et de CentOS.

```
$ yum install vsftpd
```

Créer l'utilisateur

Créer un utilisateur install pour le serveur local. Cet utilisateur n'est pas censé se connecter directement au système. Les fichiers seront stockées en-dessous de /srv/ftp/install, le répertoire utilisateur correspondant qu'on doit créer au préalable.

```
$ mkdir -pv -m 0770 /srv/ftp/install
```

```
mkdir: created directory ‘/srv/ftp’
mkdir: created directory ‘/srv/ftp/install’
```

```
$ useradd -c "G4L User" -d /srv/ftp/install -s /sbin/nologin install
```

```
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
```

```
  $ chown -R install:install /srv/ftp/install/
  $ passwd install
```

```
  Changing password for user install.
  New password: **********
  Retype new password: **********
  passwd: all authentication tokens updated successfully.
```

Configurer le serveur

La configuration de VsFTPd s'effectue dans le fichier /etc/vsftpd/vsftpd.conf. Avant d'aller plus loin, sauvegarder la configuration par défaut.

```
$ cd /etc/vsftpd/
$ cp vsftpd.conf vsftpd.conf.orig
```

Modifier ou ajouter quelques directives. Pour commencer, désactiver les connexions anonymes.

```
anonymous_enable=NO
```

Ensuite, descendre vers la fin du fichier et définir la configuration de notre utilisateur.

```
chroot_local_user=YES
userlist_enable=YES
userlist_deny=NO
check_shell=NO
userlist_file=/etc/vsftpd/vsftpd.user_list
allow_writeable_chroot=YES
```

- **chroot*local*user=YES** interdit aux utilisateurs de quitter l'arborescence de leur répertoire utilisateur pour se balader un peu partout dans le système.
- **userlist_enable=YES** active une liste d'utilisateurs. Dans la configuration par défaut, la liste spécifie les utilisateurs auxquels on interdit l'accès au serveur. l'utilisation de **userlist_deny=NO** et d'une liste qui contient les seuls utilisateurs autorisés permet de faire le contraire.
- **check_shell=NO** est nécessaire lorsqu'un utilisateur doit pouvoir se connecter alors même qu'il ne dispose d'aucun shell de connexion.
- **userlist_file** spécifie le fichier qui contiendra la liste des utilisateurs autorisés à se connecter.

Pour autoriser les listings récursifs:

```
  ls_recurse_enable=YES
```

Le serveur utilise uniquement l'IPv4:

```
listen=YES
```

```
listen_ipv6=NO
```

Activer le mode FTP passif et définir la plage de ports dynamiques.

```
pasv_enable=YES
pasv_min_port=50001
pasv_max_port=50010
```

Étant donné qu'un utilise le mode FTP passif, on peut commenter ou supprimer la ligne suivante.

```
# connect_from_port_20=YES
```

Un peu plus bas, on pourra supprimer le doublon userlist_enable=YES et désactiver l'utilisation des encapsuleurs TCP.

```
 tcp_wrappers=NO
```

Il ne reste plus qu'à créer le fichier /etc/vsftpd/vsftpd.user_list contenantla liste des utilisateurs autorisés à se connecter à VsFTPd.

```
$ echo install > /etc/vsftpd/vsftpd.user_list
```

Mise en service et premier test

Activer et démarrer le serveur VsFTPd.

```
$ systemctl enable vsftpd
$ systemctl start vsftpd
```

Tester le serveur localement

On peut utiliser un client FTP comme ncftp ou lftp.

Avant de le lancer, on va lui fournir un fichier test.

```
$ echo "Ceci est un test FTP" > /srv/ftp/install/test
$ chown install:install /srv/ftp/install/test
```

À présent, on peut initier une connexion en tant qu'utilisateur install.

```
$ ncftp -u install localhost
```

```
  NcFTP 3.2.5 (Feb 02, 2011) by Mike Gleason
```

```
(http://www.NcFTP.com/contact/).
Copyright (c) 1992-2011 by Mike Gleason.
All rights reserved.
Connecting to localhost...
(vsFTPd 3.0.2)
Logging in...
Password requested by localhost for user "install".
Please specify the password.
Password: *********
Login successful.
Logged in to localhost.
ncftp / > ls
test
ncftp / > cat test
Ceci est un test FTP
ncftp / > bye
```

VsftpdWeb

VsftpdWeb est une interface web simple pour le serveur ftp vsftpd.

Installation des pré requis

Installation du serveur Apache

En fonction de la version de PHP requise il peut être nécessaire d'installer une version plus récente.

Désinstaller la version précédente

```
$ yum remove php php-common php-agent
```

Vérifier que les dépçots epel et remis soient activés

Un rechargement du cache yum doit faire apparaître les repos epel et remi

```
$ yum repolist
```

```
Modules complémentaires chargés : fastestmirror
Loading mirror speeds from cached hostfile
epel/metalink  21 kB 00:00
* base: centos.crazyfrogs.org
* centosplus: centos.mirror.ate.info
* contrib: centos.mirrors.ovh.net
* epel: epel.besthosting.ua
* extras: centos.crazyfrogs.org
```

```
   * remi: fr2.rpmfind.net
   * remi-safe: fr2.rpmfind.net
   * updates: centos.mirror.ate.info
```

Installer php et ses dépendances

```
$ yum install httpd php mysql-server php-mysql pam_mysql vsftpd
```

Configuration du serveur

Activer short*open*tag dans /etc/php.ini

```
short_open_tag = on
```

Si nécessaire modifier le port d'écoute du serveur

dans /etc/httpd/conf/httpd.conf

```
Listen 8080
```

Redémarrer le service httpd

```
service httpd restart
```

Télécharger la release V2

```
git clone https://github.com/Tvel/VsftpdWeb.git
```

Déplacer le dossier VsftpdWeb

Copier le fichier téléchargé dans le répertoire racine du serveur

```
mv VsftpdWeb /var/www/html
```

Créer un utilisateur juste vsftp

```
vsftpd adduser
```

Créer les répertoires FTP et xferlog.log

```
mkdir /home/vsftpd/FTP/
mkdir /home/vsftpd/xferlog.log
chmod -R 770 /home/vsftpd
chown -R vsftpd:apache /home/vsftpd
```

Créer le répertoire /etc/vsftpd/vusers

```
mkdir /etc/vsftpd/vusers
chmod 777 -R /etc/vsftpd/vusers
```

Créer la base de données vsftpd

```
mysql -u root
MariaDB [(none)]> CREATE DATABASE vsftpd;
MariaDB [(none)]> quit
```

Avant d'importer le schéma adapter vsftpd.sql

Il faut adapter les DISKs BIG1 et BIG2 à la configuration du serveur.

```
vi /var/www/html/VsftpdWeb/install_readme/vsftpd.sql
```

Par exemple si on ne veut utiliser pour les stockage que le seul répertoire /home/vsftpd

```
(5, 'disk1', '/home/vsftpd/FTP', 'BIG1'),
(6, 'disk2', '/home/vsftpd/', 'BIG2'),
(7, 'disk3', '/', 'root'),
```

Importer le schéma par défaut:

```
mysql vsftpd < /var/www/html/VsftpdWeb/install_readme/vsftpd.sql
```

ajouter un utilisateur mysql pour vsftpd

```
mysql -u root
MariaDB [(none)]>CREATE USER 'vsftpd'@'localhost' IDENTIFIED BY
'secureftp2014';
MariaDB [(none)]>GRANT ALL privileges ON vsftpd.* TO 'vsftpd'@'localhost'
IDENTIFIED BY 'secureftp2014';
MariaDB [(none)]>quit
```

Adapter le fichier de configuration database.php

```
vi /var/www/html/VsftpdWeb/application/config/database.php
```

Modifier les valeurs de $db['default']['username'] et $db['default']['password']

```
$active_group = 'default';
$active_record = TRUE;
$db['default']['hostname'] = 'localhost';
$db['default']['username'] = 'vsftpd';
$db['default']['password'] = 'secureftp2014';
$db['default']['database'] = 'vsftpd';
$db['default']['dbdriver'] = 'mysql';
$db['default']['dbprefix'] = '';
```

```
$db['default']['pconnect'] = TRUE;
$db['default']['db_debug'] = TRUE;
$db['default']['cache_on'] = FALSE;
$db['default']['cachedir'] = '';
$db['default']['char_set'] = 'utf8';
$db['default']['dbcollat'] = 'utf8_general_ci';
$db['default']['swap_pre'] = '';
$db['default']['autoinit'] = TRUE;
```

Maintenant l'interface Web devrait fonctionner. mot de passe par défaut est admin.

Configurer le service PAM

Pluggable **A**uthentication **M**odules (**PAM**) est un système permettant d'intégrer simplement divers stratégies liées à l'authentification.

Pour que **PAM** utilise la base de données il utilise pour sa configuration un dossier, `/etc/pam.d/`, comportant les fichiers de configuration des services qui l'utilisent. Un fichier `/etc/pam.d/vsftpd` existe déjà, mais il n'est pas utilisé dans son intégralité. Voici donc le contenu complet que ce fichier doit avoir:

```
$ vi /etc/pam.d/vsftpd
```

```
   #%PAM-1.0
   auth sufficient pam_unix.so
   account sufficient pam_unix.so
   session required /lib64/security/pam_mysql.so verbose=1 user=vsftpd
passwd=secureftp2014 host=127.0.0.1 db=vsftpd table=accounts
usercolumn=username passwdcolumn=pass crypt=3
   auth required /lib64/security/pam_mysql.so verbose=1 user=vsftpd
passwd=secureftp2014 host=127.0.0.1 db=vsftpd table=accounts
usercolumn=username passwdcolumn=pass crypt=3
   account required /lib64/security/pam_mysql.so verbose=1 user=vsftpd
passwd=secureftp2014 host=127.0.0.1 db=vsftpd table=accounts
usercolumn=username passwdcolumn=pass crypt=3
```

adapter **user=vsftpd passwd=secureftp2014** par ceux définis lors de la création de la base de données.

Configurer le vhost

Copier le fichier vsftpd.conf

```
mv /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.old
cp /var/www/html/VsftpdWeb/install_readme/vsftpd.conf /etc/vsftpd/
```

Adapter le fichier vsftpd.conf

Editer le fichier

```
vi /var/www/html/VsftpdWeb/install_readme/vsftpd.conf
```

Modifier si nécessaire les dernières lignes

```
guest_username=vsftpd
local_root=/home/vsftpd/FTP/$USER
user_config_dir=/etc/vsftpd/vusers
xferlog_file=/home/vsftpd/xferlog.log
```

Modifier sudoers

```
$ visudo
```

Ajouter

```
apache ALL = NOPASSWD: /bin/chown root /etc/vsftpd/vusers/[a-zA-Z0-9]*
apache ALL = NOPASSWD: /bin/rm /etc/vsftpd/vusers/[a-zA-Z0-9]*
```