LIGNIERE
Timothée
Classe
Date de création
25/02/2024
Date de maj

FTP

Sommaire

1 - Problématique

Pour de multiples raisons, il peut être nécessaire d'avoir un service permettant de transférer des fichiers de machines en machines. Il existe de multiples solutions à cela ; TFTP, FTP, SCP et SFTP.

Nous nous concentrerons sur FTP puis mettrons en place un chiffrement par SSL/TLS.

La différence majeure du FTP au TFTP est que le premier utilise le protocole TCP, là où le deuxième utilise le protocole UDP. Surprenamment, le TFTP reste le plus lent des deux en plus de ne pas assurer l'intégrité des paquets envoyés.

2 - Notice d’installation

2.1 – Installation du paquet

Installer le paquet « vsftpd » pour commencer l’installation :

```
sudo apt update
sudo apt install vsftpd
```

Vérifier que le paquet est bien actif :

```
sudo systemctl status vsftpd
```

Vous devriez avoir le retour « active(running) » si ce n’est pas le cas, activer le service :

```
sudo systemctl enable --now vsftpd
```

2.2 – Configuration du pare-feu

FTP utilise le port 20 pour son mode actif, 21 pour écouter les commandes et une fourchette de ports pour son mode passif allant de 5000 à 10000. Si vous avez en tête de configurer le chiffrement, ouvrez aussi le port 990.

```
sudo ufw allow 20/tcp
sudo ufw allow 21/tcp
sudo ufw allow 990/tcp
sudo ufw allow 5000:10000/tcp
```

2.3 – Configurer les utilisateurs

Il y a deux grands types d'utilisations d'un serveur FTP, les deux influencent la configuration du serveur :

- Vous souhaitez héberger un serveur FTP public et un grand nombre d'utilisateurs publics si connecteront.
- Vous souhaitez avoir un serveur FTP privé et ne souhaitez pas avoir d'utilisateurs publics

Dans le premier cas, vous aurez besoin de créer un utilisateur additionnel et de partager ses identifiants aux clients du serveur. Tout est identique pour le deuxième cas.

L'idée est que l'administrateur du FTP peut accéder à n'importe quel dossier du serveur et que les utilisateurs soient restreints à un seul dossier. Il est donc nécessaire d'avoir une compréhension basique des droits sous Linux.

Pour commencer, créer votre utilisateur public :

```
sudo adduser ftpuser
```

Pour des questions de sécurité, désactiver les connexions ssh sur cet utilisateur :

```
sudo nano /etc/ssh/sshd_config
```

Puis rajouter :

```
DenyUsers ftpuser
```

Sauvegarder, quitter puis redémarrer le service sshd :

```
sudo systemctl restart sshd
```

2.4 – Créer le dossier FTP et établir les permissions

Créer le dossier qui servira pour le service FTP :

```
sudo mkdir /srv/ftp
```

Désormais changer la propriété du dossier par votre utilisateur administrateur :

```
sudo chown <ADMIN USER> /srv/ftp
```

2.5 – Configurer et sécuriser vsftpd

Ouvrez le fichier de configuration de vsftpd

```
sudo nano /etc/vsftpd.conf
```

Assurez-vous que les lignes suivantes soient décommentés :

```
anonymous_enable=NO
local_enable=YES
write-enable=YES
```

Ayant ouvert les ports 5000 à 10000 précédemment, pensez à les préciser dans le fichier de configuration :

```
pasv_min_port=5000
pasv_max_port=10000
```

Préciser le dossier du serveur FTP :

```
local_root=/srv/ftp
```

Bloquer les utilisateurs à ce dossier :

```
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
allow_writeable_chroot=YES
```

Paramétrer le masque de droits :

```
local_umask=0002
```

Ce masque équivaut aux droits 664 (-rw-rw-r-) et tout nouveaux dossiers à 775(rwxrwxr-x). Paramétrer ainsi, ftpuser n'aura pas le droits d'importer des dossiers/fichiers sur notre serveur FTP. Vous pouvez modifier cela si vous le souhaitez.

Puis créer la liste que nous avons précisée dans le fichier de configuration :

```
sudo touch /etc/vsftpd.chroot_list
sudo nano /etc/vsftpd.chroot_list
```

Tous les utilisateurs précisés dans ce fichier ne sera pas restreint par le service.

Enfin, redémarrer le serveur FTP pour appliquer les nouveaux paramètres :

```
sudo systemctl restart vsftpd
```

2.6 – Sécuriser vsftpd avec SSL/TLS

Il est recommandé de chiffrer le trafic FTP si vous souhaitez l'utiliser depuis Internet. Nous chiffrerons notre trafic à l'aide de FTPS. Pour commencer, générons un certificat :

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
```

Remplissez les informations demandées. Une fois cela fait, retourner dans le fichier de configuration de vsftpd

```
sudo nano /etc/vsftpd.conf
```

Retirez les lignes suivantes :

```
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
```

Puis rajouter les lignes suivantes :

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

Sauvegarder puis redémarrer le service :

```
sudo systemctl restart vsftpd
```

3 - Notice d’utilisation

3.1 – Commande FTP

Si vous souhaitez vous connecter au serveur depuis un terminal, voici les commandes FTP :

ftp	Passer le terminal en mode ftp
open <IP ADDRESS>	Se connecter à un serveur
pwd	Voir le dossier actuel
cwd	Changer de dossier
dele <FILENAME>	Supprimer un fichier/dossier
cdup	Retourner au dossier racine
help	Renvoie des informations d’aide
cd	Changer de dossier
get <FILENAME>	Télécharger un fichier/dossier
put <FILENAME>	Envoyer un fichier/dossier
bye	Terminer la session FTP

4 - Annexes

Fiche de recette

Vérification de l'opérationnalité de la solution mise en œuvre : *FTP*

Description du test :

1. *Vérifier statut du service*
2. *Envoyer un fichier*
3. *Recevoir fichier*

Résultats Attendus :

1. *Service en active(running)*
2. *Fichier bien reçu sur le serveur FTP*
3. *Fichier bien reçu sur le client*

Réception Globale : FTP **Auteurs: Lignière Timothée**	**Date: *25/02/2024***
Reçu : ☐	
Reçu avec réserve : ☐ ……	
Refusé : ☐……	
Commentaire :	

Recette étape par étape * — ****** (pour chaque étape, vous devez élaborer dans un fichier distinct un scénario détaillé à faire appliquer au « client » venant valider votre solution)*

Réception Etape 1: Faire la commande sudo systemctl status vsftpd et s'assurer d'avoir le résultat active(running) dans le statut du service
Reçu : ☐
Reçu avec réserve : ☐……
Refusé : ☐……
Commentaire :

Réception Etape 2 : *Envoyer un fichier depuis le client sur le serveur FTP qu'importe la méthode utilisée*
Reçu : ☐
Reçu avec réserve : ☐……
Refusé : ☐……
Commentaire :

Réception Etape 3 : *Récupérer un fichier sur le serveur FTP depuis un client qu'importe la méthode utilisée*
Reçu : ☐
Reçu avec réserve : ☐……
Refusé : ☐……
Commentaire :