

ATELIER N°5 : Mise en place d'un serveur FTP

INTRODUCTION

Le protocole FTP (File Transfer Protocol) permet le transfert de fichiers entre un client et un serveur. Il est utilisé pour partager des fichiers au sein d'un réseau local ou via Internet. Toutefois, FTP classique n'est pas sécurisé, d'où l'existence de variantes comme FTPS (FTP sécurisé avec TLS) et SFTP (FTP via SSH).

Dans cette documentation, nous allons installer et configurer un serveur FTP en utilisant ProFTPD, un serveur FTP léger et performant.

Première partie : Installation et configuration de base Nous installerons ProFTPD, vérifierons son bon fonctionnement et testerons une connexion FTP avec un utilisateur standard. Nous nous assurerons également que cet utilisateur ne puisse pas accéder en dehors de son répertoire personnel.

Deuxième partie : Configuration de l'accès anonyme Nous permettrons aux utilisateurs anonymes d'accéder en lecture aux fichiers du serveur FTP, avec une configuration spécifique pour garantir la sécurité et éviter toute modification ou suppression de fichiers par ces utilisateurs.

Troisième partie : Mise en place de VirtualHosts pour l'Intranet et l'Extranet Nous configurerons deux serveurs FTP distincts : Un serveur pour l'Intranet (accès interne) avec une adresse IP spécifique et un port dédié. Un serveur pour l'Extranet (accès externe) avec une autre adresse IP et un autre port. Nous utiliserons des interfaces réseau virtuelles pour séparer ces services et affecter chaque utilisateur à son environnement de travail.

PREMIERE PARTIE

Premierement nous allons commencer par copier notre template de base ,pour avoir un nouveau container dans laquelle il faudra definir une nouvelle adresse ip qui sera 10.31.80.20 pour le premier binome et 10.31.81.21 pour le deuxieme binome 10.31.80.20.

```
lxc-copy -n template -N ftp2
```

```
nano /etc/network/interfaces
```

ensuite nous allons installer proftpd

```
sudo apt update && sudo apt install proftpd -y
```

ensuite nous pouvons voir que le port par défaut de proftpd est le 21 grâce à la commande :

```
netstat -nautp
```

```
root@ftp1:~# netstat -nautp
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat PID/Program name
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 86/sshd: /usr/sbin/
tcp6 0 0 :::21 :::* LISTEN 388/proftpd: (accep
tcp6 0 0 :::22 :::* LISTEN 86/sshd: /usr/sbin/
```

Pour empêcher l'utilisateur de sortir de son répertoire il faut ajouter cette ligne ou la décommenter dans le fichier

```
nano /etc/proftpd/proftpd.conf
```

```
DefaultRoot ~
```

dans le même fichier pour activer les virtual hosts, il faut dé-commenter la ligne

```
#Include /etc/proftpd/virtuals.conf
```

DEUXIEME PARTIE

Pour permettre aux utilisateurs anonymes de se connecter, nous avons décommenté les lignes anonymous et on y a ajouté le dossier dans lequel les comptes pourront se connecter. Mais pour des travaux futurs ils seraient préférable de directement copier coller les lignes de commandes ci-dessous en toute fin du fichier ftpdocs.

```
nano /etc/proftpd/proftpd.conf
```

```
<Anonymous /home/ftpdocs>
  User ftp
  Group nogroup
  # We want clients to be able to login with "anonymous" as well as "ftp"
  UserAlias anonymous ftp
  # Cosmetic changes, all files belongs to ftp user
  DirFakeUser on ftp
  DirFakeGroup on ftp

  RequireValidShell off

  # Limit the maximum number of anonymous logins
  MaxClients 10

  # We want 'welcome.msg' displayed at login, and '.message' displayed
  # in each newly chdir'd directory.
  DisplayLogin welcome.msg
  DisplayChdir .message

  # Limit WRITE everywhere in the anonymous chroot
  <Directory *>
    <Limit WRITE>
```

```
    DenyAll
  </Limit>
</Directory>

# Uncomment this if you're brave.
# <Directory incoming>
#   # Umask 022 is a good standard umask to prevent new files and dirs
#   # (second parm) from being group and world writable.
#   Umask 022 022
#   <Limit READ WRITE>
#     DenyAll
#     </Limit>
#     <Limit STOR>
#       AllowAll
#     </Limit>
# </Directory>

</Anonymous>
```

TROISIEME PARTIE

Dans cette troisieme partie nous allons commencer par configurer les deux virtualshost en ajoutant des interfaces pour intra et extra dans le fichier interfaces

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 10.31.80.21/20
    gateway 10.31.95.254
    dns-nameservers 10.31.80.53 10.31.80.54

auto eth0:0
iface eth0:0 inet static
    address 10.31.80.12
    netmask 255.255.240.0

auto eth0:1
iface eth0:1 inet static
    address 10.31.80.13
    netmask 255.255.240.0
```

Il faut aussi ajouter certaine modifications dans le fichier virtuals conf pour declarer les deux vhost

```
nano /etc/proftpd/virtuals.conf <\code>
```

```
<code>
<VirtualHost 10.31.81.12>
    ServerAdmin admin@m2l.org
    ServerName "FTP INTRANET"
    User intra
    Group intra
    Port 2100
    # Pour n'autoriser que le groupe intra
    <Limit LOGIN>
        Order Allow,Deny
        Allowgroup intra
        Deny from all
    </Limit>
    Umask 022
    TransferLog /var/log/proftpd/xfer/ftp-intranet.m2l.org
    MaxLoginAttempts 10
    DefaultRoot /srv/ftp/intranet
    AllowOverwrite yes
</VirtualHost>
<VirtualHost 10.31.81.13>
    ServerAdmin admin@m2l.org
    ServerName "FTP INTRANET"
    User extra
    Group extra
    Port 2200
    # Pour n'autoriser que le groupe extra
    <Limit LOGIN>
        Order Allow,Deny
        Allowgroup extra
        Deny from all
    </Limit>
    Umask 022
    TransferLog /var/log/proftpd/xfer/ftp-extranet.m2l.org
    MaxLoginAttempts 10
    DefaultRoot /srv/ftp/extranet
    AllowOverwrite yes
</VirtualHost>
<\code>
```

Les interfaces crée il faut creer les deux utilisateur intra et extra\\

```
<code>
sudo adduser intra
sudo adduser extra
```

Ensuite il faut creer les dossier pour chaque utilisateur

```
sudo mkdir -p /srv/ftp/intranet
sudo mkdir -p /srv/ftp/extranet
```

Et pour finir il faut donner les permissions de dossier au deux utilisateurs

```
sudo chmod 755 /srv/ftp/extranet
sudo chmod 750 /srv/ftp/intranet
```

Maintenant les deux virtual host sont configurés et chaque utilisateur a son propre dossier, l'utilisateur extra peut lire et exécuter, mais pas écrire et l'utilisateur intra lui peut lire, exécuter et écrire.

QUATRIEME PARTIE

Dans cette quatrième partie nous remarquons bien que les informations circulent en clair (non chiffré) entre le client et le serveur ici entre 10.31.80.20 et 10.187.20.202.

No.	Time	Source	Destination	Protocol	Length	Info
39	12.902281	10.31.80.20	10.187.20.202	FTP	102	Response: 220 ProFTPD Server (ftpl) [::ffff:10.31.80.20]
40	12.902375	10.187.20.202	10.31.80.20	FTP	64	Request: AUTH TLS
42	12.905049	10.31.80.20	10.187.20.202	FTP	86	Response: 500 commande AUTH non comprise
43	12.906198	10.187.20.202	10.31.80.20	FTP	64	Request: AUTH SSL
44	12.909549	10.31.80.20	10.187.20.202	FTP	86	Response: 500 commande AUTH non comprise
46	14.700193	10.187.20.202	10.31.80.20	FTP	64	Request: USER std
47	14.707487	10.31.80.20	10.187.20.202	FTP	88	Response: 331 Mot de passe requis pour std
48	14.707758	10.187.20.202	10.31.80.20	FTP	69	Request: PASS password
49	14.745313	10.31.80.20	10.187.20.202	FTP	88	Response: 230 Utilisateur std authentifié
50	14.745750	10.187.20.202	10.31.80.20	FTP	60	Request: SYST
51	14.748906	10.31.80.20	10.187.20.202	FTP	73	Response: 215 UNIX Type: L8
52	14.749256	10.187.20.202	10.31.80.20	FTP	60	Request: FEAT

From:

<https://sisr2.beaupeyrat.com/> - Documentations SIO2 option SISR

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr1-g5:ftp>

Last update: **2025/04/08 10:29**

