

Compte rendu d'Installation « Serveur ProFTP »

Table des matières

Objectif(s) :.....	2
Légende :	2
Installation du serveur ProFTPD.....	3
Les utilisateurs.....	3
Accès en anonyme.....	3
Configuration général.....	4
Configuration avec keepalived :	9

Objectif(s) :

L'objectif de ce tuto est de configurer un serveur FTP, de faire des injections MYSQL et de configurer notre MYSQL et de configurer notre serveur FTP avec Keepalived.

Légende :

- Les commandes ou les chemins (absolue/relatif) sont en gras, souligné et en italique ex :
 - *Apt-get update*
- Des captures d'écrans ont été prises afin de faciliter la compréhension du lecteur.

Machine	Os	Distribution	Version	C/S	IP
POSTE21	Debian	Linux	8.5	S	192.168.1.140

Un serveur FTP permet de stocker des fichiers, des répertoires et de mettre ceux-ci à la disposition des clients. Deux catégories de clients sont à considérer : les utilisateurs authentifiés avec noms et mots de passe d'une part et les anonymes d'autre part. Les utilisateurs ont le droit de déposer et de charger des fichiers à partir de leur répertoire personnel sur le serveur. Les anonymes ne peuvent que charger des documents du serveur vers leur machine.

Proftp utilise une syntaxe similaire à celle d'Apache permettant ainsi d'homogénéiser les fichiers de configurations.

Installation du serveur ProFTPD.

apt install proftpd

Paramétrer le serveur en mode standalone. (Indépendamment)

Les utilisateurs

Attention, tous les utilisateurs se connectant sur le serveur Proftp doivent exister réellement sur le système (avec un UID).

Accès en anonyme

Il faut créer la section anonymous pour que les clients puissent se connecter sans authentification, en fait au nom de l'utilisateur ftp, dont le répertoire personnel est /home/ftp, et qui n'a pas de shell, comme le confirme l'examen de /etc/passwd.

```
GNU nano 2.2.6 Fichier : proftpd.conf
<Anonymous ~ftp>
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 chdired 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>

# Include other custom configuration files
Include /etc/proftpd/conf.d/
```

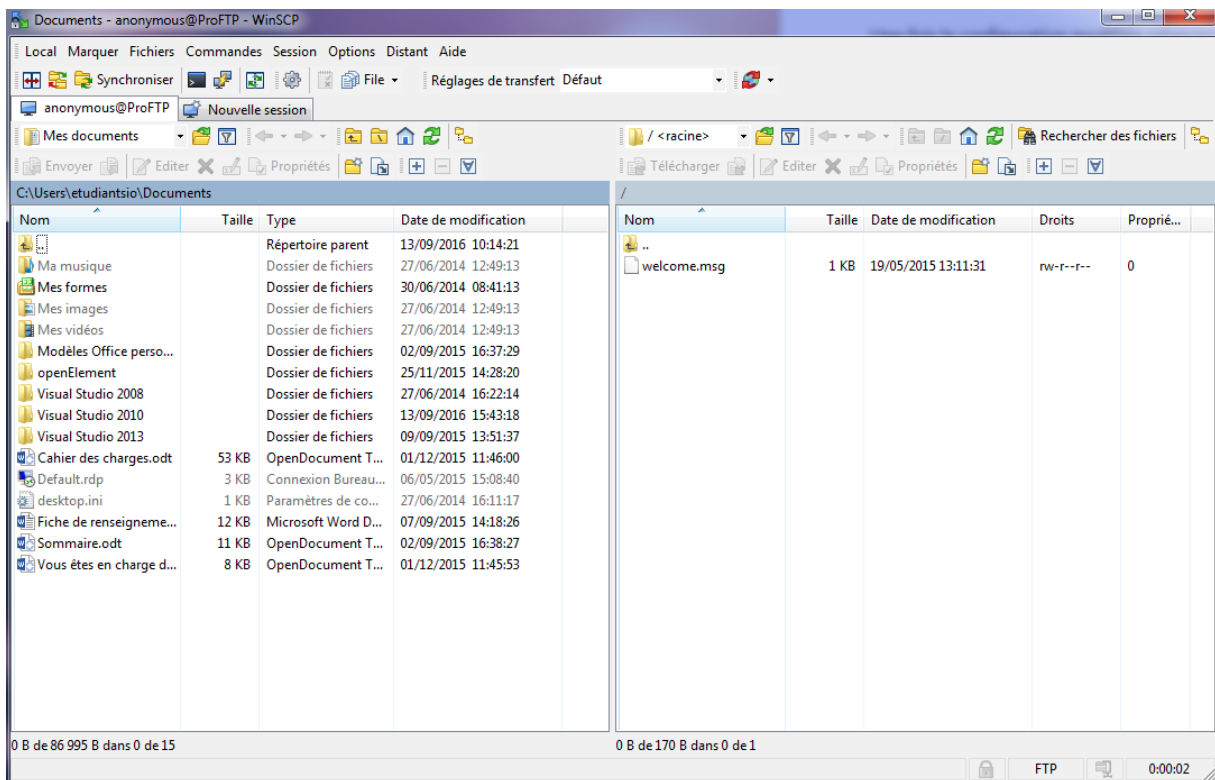
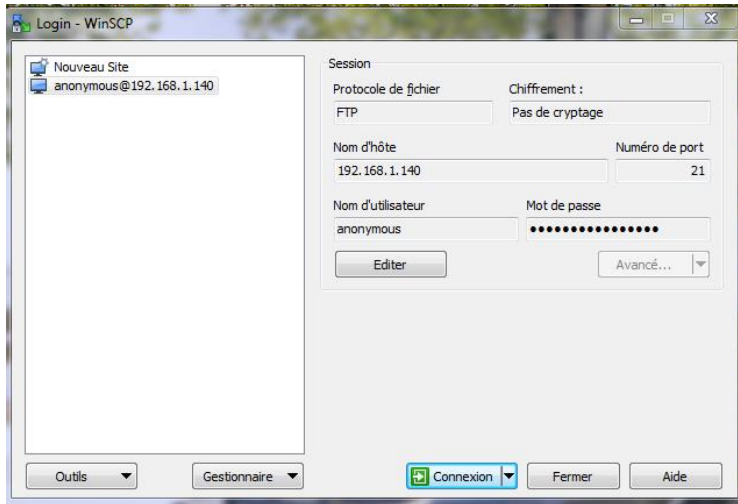
Une fois la configuration modifiée relancez le serveur.

reboot

Configuration général

Le fichier de configuration est [/etc/proftpd/proftp.conf](#).

J'utilise WinSCP pour tester l'accès au serveur ftp.



On remarque que l'on accède à notre serveur.

On va ensuite paramétrer le mode passif (ports 63000 à 65000), Afin le serveur fournisse le numéro de port au client sinon on est bloqué par les par feux, dans le fichier de configuration proftpd.conf.

```
PassivePorts 63000 65000
```

On va installer Apache et donner des droits avec un utilisateur qui s'appellera Toto.




ap-get install apache2

```
root@ProFTP:/var/www# adduser letort
Ajout de l'utilisateur « letort » ...
Ajout du nouveau groupe « letort » (1001) ...
Ajout du nouvel utilisateur « letort » (1001) avec le groupe « letort » ...
Création du répertoire personnel « /home/letort »...
Copie des fichiers depuis « /etc/skel »...
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur letort
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
  Nom complet []:
  N° de bureau []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Cette information est-elle correcte ? [O/n]o
root@ProFTP:/var/www# cd /home/letort/
root@ProFTP:/home/letort# ls -l
total 0
root@ProFTP:/home/letort# mkdir public_html
root@ProFTP:/home/letort# ls -l
total 4
drwxr-xr-x 2 root root 4096 sept. 26 09:19 public_html
root@ProFTP:/home/letort# cd public_html/
root@ProFTP:/home/letort/public_html# test.html
-bash: test.html : commande introuvable
root@ProFTP:/home/letort/public_html# touch test.html
root@ProFTP:/home/letort/public_html# ls -l
total 0
-rw-r--r-- 1 root root 0 sept. 26 09:19 test.html
```

On va maintenant permettre l'accès au répertoire public_html, pour l'utilisateur letort.

```
root@ProFTP:/home# chown -R "letort:letort" "/home/letort"
root@ProFTP:/home# ls -l
total 24
drwxr-xr-x 2 adrien adrien 4096 sept. 15 10:32 adrien
drwxr-xr-x 3 letort letort 4096 sept. 26 09:19 letort
drwx----- 2 root root 16384 sept. 15 09:32 lost+found
root@ProFTP:/home# cd letort/
root@ProFTP:/home/letort# ls -l
total 4
drwxr-xr-x 2 letort letort 4096 sept. 26 09:19 public_html
```

On va mettre le script dans le home letort à l'aide de winscp

Nom	Taille	Date de modification	Droits
 /home/letort/public_html			
 proftpd_mysql.txt	3 KB	10/03/2014 10:09:32	rw-r--r--
 test.html	0 KB	26/09/2016 09:19:20	rw-r--r--

Installation de mysql-server et proftpd mod mysql :

```
apt-get install mysql-server
```

```
root@ProFTP:/home# apt-get install proftpd-mod-mysql
```

```
# mysql -u root -p
```

Voir les bases de données :

```
#show databases ;
```

```
#create database proftpd
```

```
#grant select, insert, update, delete on proftpd.* to 'proftpd'@'localhost' identified by 'root';
```

```
#flush privileges;
```

```
#quit;
```

On va maintenant pouvoir insérer le script :

```
#mysql -u root -p proftpd < /home/letort/public_html/proftpd_mysql.txt
```

```
#mysql -u proftpd -p
```

```
#show databases;
```

```
#use proftpd;
```

```
#show tables;
```

```
#desc ftpgroup;
```

```
#desc ftpusers;
```

```
#quit;
```

Paramétrer proftpd.conf :

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

Décommentez le Include /etc/proftpd/sql.conf

```
include /etc/proftpd/sql.conf
```

```
#nano /etc/proftpd/modules.conf
```

Il faut décommenter ces lignes :

```
#loadModule mod_sql.c
```

```
#loadModule mod_sql_mysql.c
```

```
192.168.1.140 - PuTTY
GNU nano 2.2.6 Fichier : modules.conf

#
# This file is used to manage DSO modules and features.
#
# This is the directory where DSO modules reside
ModulePath /usr/lib/proftpd

# Allow only user root to load and unload modules, but allow everyone
# to see which modules have been loaded

ModuleControlsACLs inssmod,rmmod allow user root
ModuleControlsACLs lsmod allow user *

LoadModule mod_ctrls_admin.c
LoadModule mod_tls.c

# Install one of proftpd-mod-mysql, proftpd-mod-pgsql or any other
# SQL backend engine to use this module and the required backend.
# This module must be mandatory loaded before anyone of
# the existent SQL backends.
LoadModule mod_sql.c

# Install proftpd-mod-ldap to use this
#LoadModule mod_ldap.c

#
# 'SQLBackend mysql' or 'SQLBackend postgres' (or any other valid backend) directives
# are required to have SQL authorization working. You can also comment out the
# unused module here, in alternative.
#

# Install proftpd-mod-mysql and decomment the previous
# mod_sql.c module to use this.
LoadModule mod_sql_mysql.c
```

Dans */proftpd/sql.conf*

```
192.168.1.140 - PuTTY
GNU nano 2.2.6 Fichier : sql.conf

#
# Proftpd sample configuration for SQL-based authentication.
#
# (This is not to be used if you prefer a PAM-based SQL authentication)
#
<IfModule mod_sql.c>
#
# Choose a SQL backend among MySQL or PostgreSQL.
# Both modules are loaded in default configuration, so you have to specify the backend
# or comment out the unused module in /etc/proftpd/modules.conf.
# Use 'mysql' or 'postgres' as possible values.
#
SQLBackend      mysql
#
SQLEngine on
SQLAuthenticate users groups
#
# Use both a crypted or plaintext password
SQLAuthTypes Crypt
#
# Use a backend-crypted or a crypted password
#SQLAuthTypes Crypt
#
# Connection
SQLConnectInfo proftpd@localhost proftpd root
#
# Describes both users/groups tables
#
SQLUserInfo ftpuser userid passwd uid gid homedir shell
#SQLUserwhereClause "loginallowed = 'true'"

SQLGroupInfo ftpgroup groupname gid members

#Pour créer le repertoire utilisateur qd il va se connecter
CreateHome on
#
</IfModule>
```

On va ensuite restart :

```
# systemctl restart proftpd

#groupadd -g 5500 ftpgroup

#useradd -u 5500 -s /bin/false -d /bin/null -g ftpgroup ftpuser

#cat etc/passwd

#gpasswd -a ftpuser ftpgroup
```

On va maintenant créer un utilisateur titi pour se connecter avec un utilisateur qu'on a créé dans mysql :

```
# mysql -u proftpd -p proftpd

#insert into ftpgroup values ('ftpgroup',5500,'ftpuser');

#select * from ftpgroup;

#insert into ftpuser values (1,'titi',encrypt('secret'),5500,5500,' /home/titi', ' /sbin/nologin', '','', '');
```

```
mysql> insert into ftpuser values (1,'titi',encrypt('secret'),5500,5500,' /home/letort', ' /sbin/nologin','', '','');
ERROR 1062 (23000): Duplicate entry '1' for key 'PRIMARY'
mysql> insert into ftpuser values (2,'titi',encrypt('secret'),5500,5500,' /home/letort', ' /sbin/nologin','', '','');
Query OK, 1 row affected, 4 warnings (0.00 sec)
```

On peut voir si tout a été créé, :

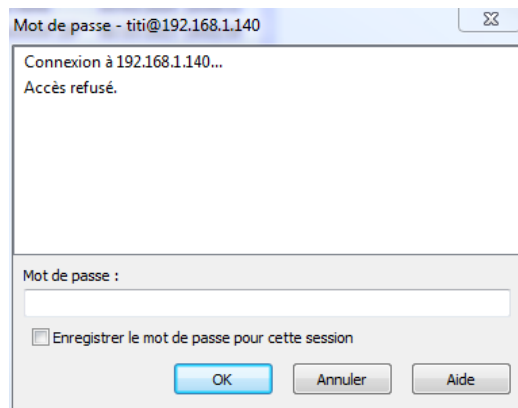
```
#select * from ftpuser
```

```
mysql> select * from ftpuser;
```

id	userid	passwd	uid	gid	homedir	shell	count	accessed	modified	LoginAllowed
1	letort	.EoZXstYR8ujk	5500	5500	/home/letort	/sbin/nologin	0	0000-00-00 00:00:00	0000-00-00 00:00:00	
2	titi	jvCF4g7PHgKvc	5500	5500	/home/titi	/sbin/nologin	0	0000-00-00 00:00:00	0000-00-00 00:00:00	
3	toto	GcNVFphUsVitI	5500	5500	/home/toto	/sbin/nologin	0	0000-00-00 00:00:00	0000-00-00 00:00:00	

3 rows in set (0.00 sec)

On va se co a winscp :



Lorsqu'on regarde dans mysql les ftpusers on remarque que le homedir n'est peut être pas mis correctement : si c'est le cas, changeons-le. :


```
mysql> update ftpuser set homedir='/home/titi' where id=2;
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from ftpuser;
+----+-----+-----+-----+-----+-----+-----+-----+
| id | userid | passwd          | uid | gid | homedir        | shell          | c
+----+-----+-----+-----+-----+-----+-----+-----+
|  1 | letort | .EoZXstYR8ujk  | 5500 | 5500 | /home/letort   | /sbin/nologin |
|  2 | titi   | jvCF4g7PHgKvc | 5500 | 5500 | /home/titi     | /sbin/nologin |
+----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

On va ensuite cloner la VM ProFTP et la nommer ProFTP2 et on ne va pas oublier de changer le hostname dans */etc/hostname* et le host dans */etc/hosts*

Configuration avec keepalived :

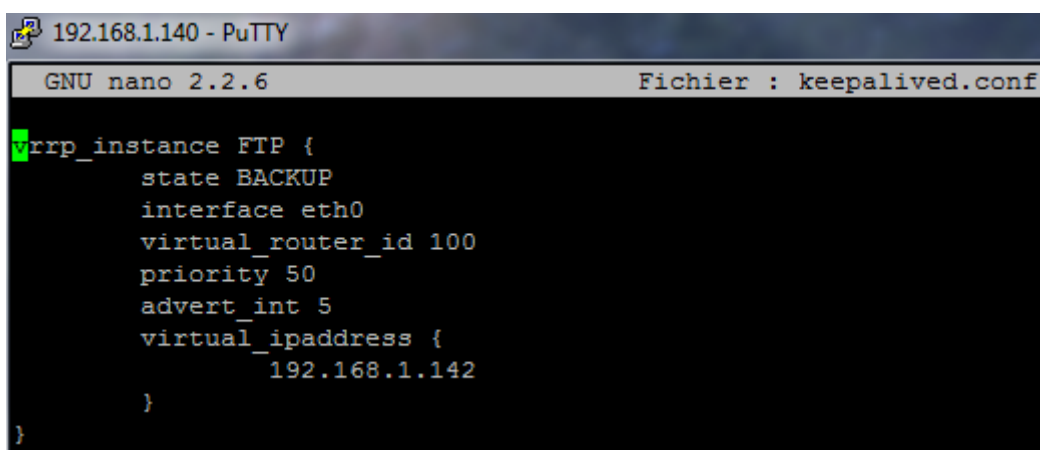
On va commencer par installer keepalivd sur les deux machines :

```
#apt-get install keepalived
```

On va ensuite configurer le fichier qu'on va créer et mettre le minimum d'information dedans :

```
#nano /etc/keepalived/keepalived.conf
```

On va y ajouter cela :



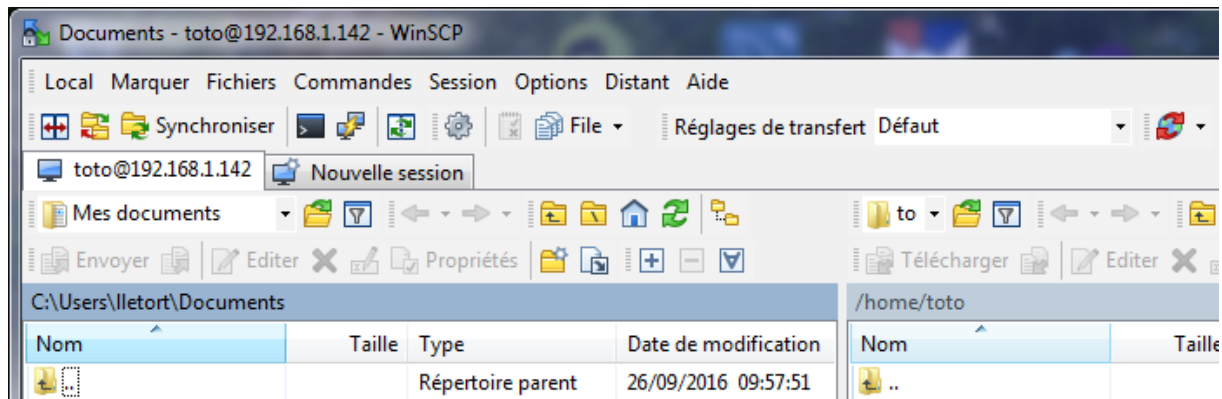
```
192.168.1.140 - PuTTY
GNU nano 2.2.6                                Fichier : keepalived.conf
vrrp_instance FTP {
    state BACKUP
    interface eth0
    virtual_router_id 100
    priority 50
    advert_int 5
    virtual_ipaddress {
        192.168.1.142
    }
}
```

Sur le deuxieme server on va mettre une priority 100

Ne pas oublier de redémarrer le service keepalived.

```
#systemctl restart keepalived
```

On va ensuite voir si on peut se connecter avec WINSCP avec les identifiants toto et secret avec l'adresse Ip virtuelle.

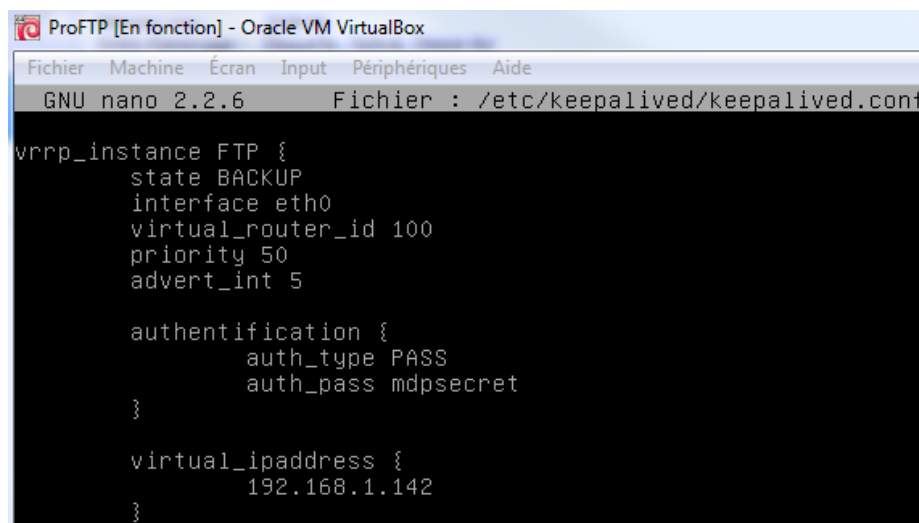


Cela marche correctement.

Ne pas oublier d'avoir des hostnames différents sur ces deux machines et d'avoir la correspondance dans le host :

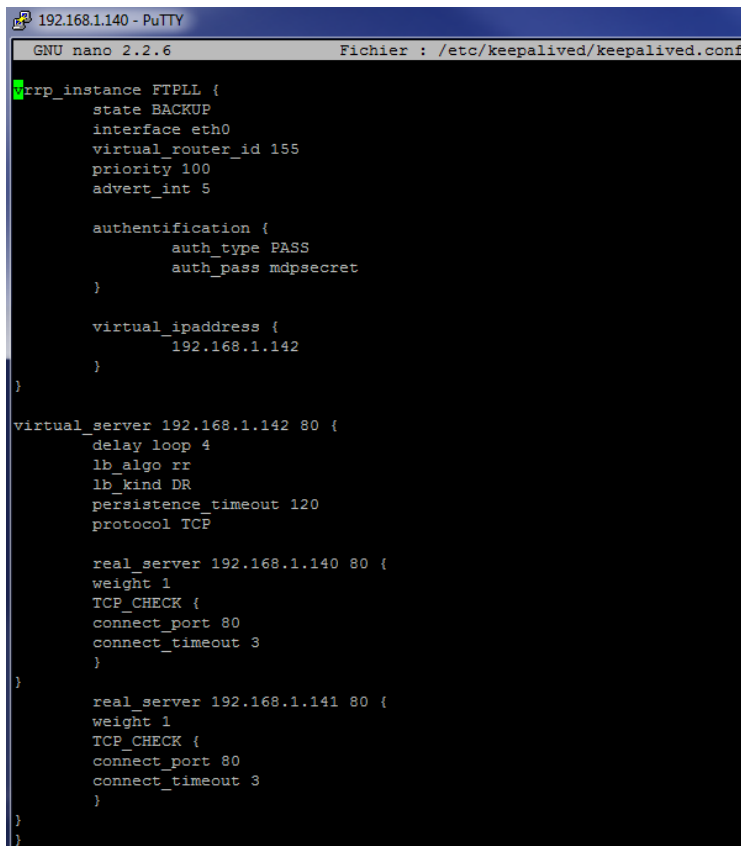
```
#/etc/hostname #/etc/hosts
```

On va mettre une authentification :



Ne pas oublier de faire un restart !

On va maintenant rajouter des lignes dans le fichier de conf `/etc/keepalived/keepalived.conf`



```
GNU nano 2.2.6 Fichier : /etc/keepalived/keepalived.conf
vrrp_instance FTPLL {
    state BACKUP
    interface eth0
    virtual_router_id 155
    priority 100
    advert_int 5

    authentication {
        auth_type PASS
        auth_pass mdpsecret
    }

    virtual_ipaddress {
        192.168.1.142
    }
}

virtual_server 192.168.1.142 80 {
    delay_loop 4
    lb_algo rr
    lb_kind DR
    persistence_timeout 120
    protocol TCP

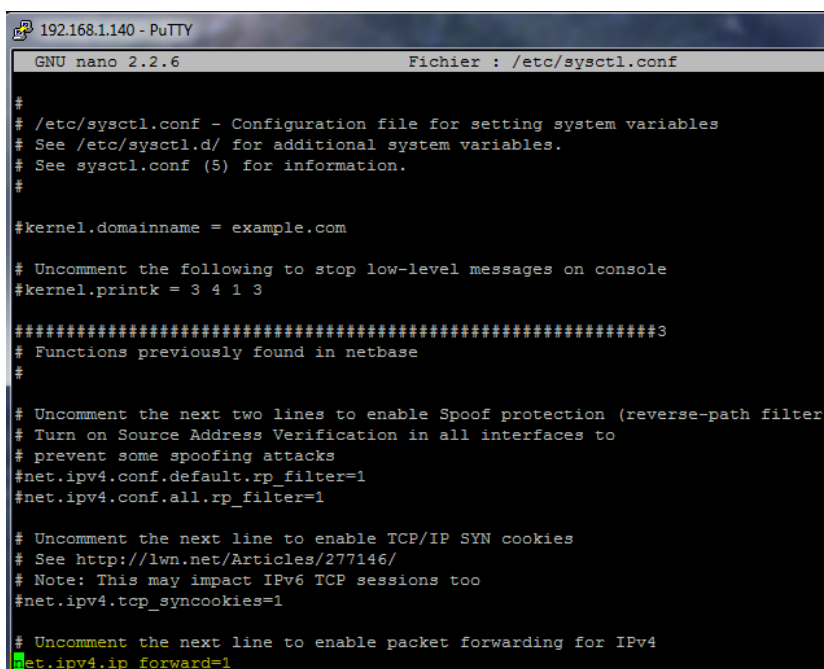
    real_server 192.168.1.140 80 {
        weight 1
        TCP_CHECK {
            connect_port 80
            connect_timeout 3
        }
    }

    real_server 192.168.1.141 80 {
        weight 1
        TCP_CHECK {
            connect_port 80
            connect_timeout 3
        }
    }
}
```

On met en port 80 pour faire des tests avec apache2 ! Sur notre navigateur :

Dans `/etc/sysctl.conf` :

Il faut dé-argumenté la dernière ligne pour permettre les Ip virtuelles.



```
GNU nano 2.2.6 Fichier : /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

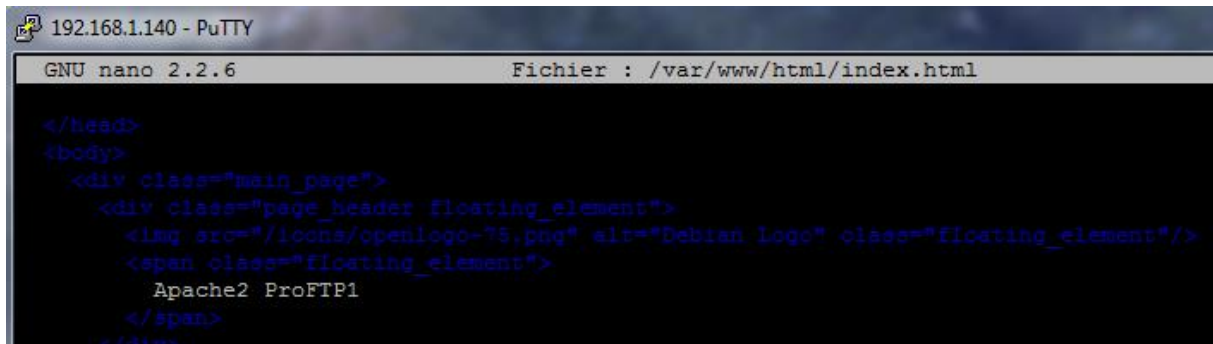
#####3
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

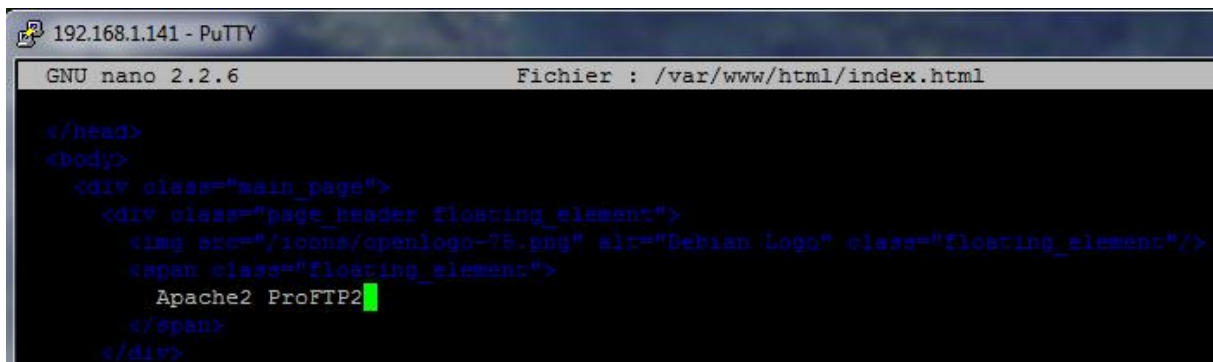
On va ensuite changer els conf d'apache2 des deux serveurs pour savoir qu'elle serveur se connecter :

```
#nano /var/www/html/index.html
```



```
192.168.1.140 - PuTTY
GNU nano 2.2.6 Fichier : /var/www/html/index.html

</head>
<body>
  <div class="main_page">
    <div class="page_header floating_element">
      
      <span class="floating_element">
        Apache2 ProFTP1
      </span>
    </div>
  </div>
```



```
192.168.1.141 - PuTTY
GNU nano 2.2.6 Fichier : /var/www/html/index.html

</head>
<body>
  <div class="main_page">
    <div class="page_header floating_element">
      
      <span class="floating_element">
        Apache2 ProFTP2
      </span>
    </div>
  </div>
```

Il faut ensuite redémarrer les deux apache2 :

```
#systemctl restart apache2
```