

FTP

Servidor Vsftpd

S'instal·la de la forma habitual (*apt install vsftpd*) i s'inicia/habilita també de la forma habitual (*systemctl start|stop vsftpd*). Els seus fitxers de configuració són:

/etc/vsftpd.conf	Fitxer de configuració principal
/etc/ftpusers	Llista d'usuaris locals del sistema no permesos per connectar al servidor FTP (cal escriure a cada línia un nom). Aquest fitxer és estàndar per diferents programes servidor però usant Vsftpd se sol fer servir el fitxer /etc/vsftpd.user_list
/etc/vsftpd.user_list	Llista d'usuaris permesos per connectar al servidor FTP (si la directiva <i>userlist_deny=NO</i>) o no permesos (si la directiva <i>userlist_deny=YES</i>). Cal crear-lo
/etc/vsftpd.chroot_list	Llista d'usuaris que en connectar només podran treballar dins de la seva carpeta personal (si la directiva <i>chroot_local_user=NO</i>) o que podran treballar a for a d'ella (si la directiva <i>chroot_local_user=YES</i>). Cal crear-lo.
/etc/pam.d/vsftpd	Fichero PAM que indica dónde se encuentran los usuarios del servidor ftp. Por defecto los usuarios son los usuarios del sistema linux. Permite configurarse para tener usuarios ftp diferentes a los usuarios del sistema (en una base de datos, en un servidor Ldap, etc).

A continuació es llisten les directives de configuració més importants del fitxer *vsftpd.conf*:

listen=YES #Activa el servidor
listen_ipv6=NO #Activa el servidor escoltant mitjançant IPv6. No compatible amb *listen*, atenció!

local_enable=YES #Activa l'ús d'usuaris locals del sistema per loguejar-se al servidor.
En qualsevol cas, aquests usuaris han de disposar d'un shell i d'una carpeta personal, que és on entraran automàticament un cop loguejats

userlist_enable=YES #Activa la lectura del fitxer /etc/vsftpd.user_list
userlist_deny=YES # Si val YES, la llista al fitxer *user_list* seran els usuaris denegats ("llista negra").
Si val NO, seran els admesos ("llista blanca")

write_enable=YES #Activa la possibilitat de pujar fitxer, per qualsevol usuari excepte anònim

chroot_local_user=YES #Estableix l'"engabiament" dels usuaris locals dins de la seva carpeta personal segons el valor de la directiva següent
chroot_list_enable=NO #Si l'anterior directiva val YES i aquesta YES, els usuaris llistats a l'arxiu /etc/vsftpd.chroot_list seran els que NO estan engabiats. Si l'anterior directiva val YES i aquesta NO, els usuaris llistats seran els que SÍ estan engabiats. Si l'anterior directiva val NO i aquesta YES, els usuaris llistats seran els que SÍ estan engabiats. Si l'anterior directiva val NO i aquesta NO, els usuaris llistats seran els que NO estan engabiats.

Altres directives que no se solen canviar respecte el seu valor per defecte són:

listen_port=21 #Port d'escolta
port_enable=YES i *pasv_enable=YES* #Activen els dos mètodes estàndar de connexió FTP
ftpd_banner="Benvingut" #També està *banner_file /ruta/fitxer/missatge*
max_clients=0 #Màxim de connexions paral·leles possibles. 0 = il·limitat

anonymous_enable=NO #Si YES, permet accés anònim (amb accés de només lectura, normalment)
Per accedir amb l'usuari anònim, hem d'escriure "anonymous" i la contrasenya no importa

```
anon_root=/carpeta/a/la/que/aniran/els/usuarios/anonims/un/cop/han/entrat (per defecte cap!)
no_anon_password=NO #Si YES, no es preguntarà cap contrasenya a l'usuari anònim (entra directe)
anon_upload_enable=NO #Si YES l'opció write_enable també ha de valer YES per a què funcioni
anon_mkdir_write_enable=NO #Per poder crear subdirectoris. " " " " " " "
anon_umask=002 #En el cas que la directiva anon_upload_enable sigui YES
anon_max_rate=0 #Màxim ample de banda (en bytes/s) permès pels anònims. 0 = il.limitat

local_root=/carpeta/a/la/que/aniran/els/usuarios/loguejats (per defecte la seva carpeta personal!)
local_umask=022 #En el cas que la directiva write_enable sigui YES
local_max_rate=0 #Màxim ample de banda (en bytes/s) permès pels usuarios. 0 = il.limitat
userlist_file=/ruta/alternativa/pel/fitxer/user_list
chroot_list_file=/ruta/alternativa/pel/fitxer/chroot_list
```

Per fer que el dimoni Vsftpd funcioni sobre TLS (i així assegurar les connexions), cal fer el següent:

1.- Crear el certificat i clau privada del servidor (quan es preguntí "Common Name" es posarà la IP del servidor):

```
openssl req -x509 -nodes -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/ssl/certs/vsftpd.crt
```

2.- Establir les següents directives a l'arxiu vsftpd.conf:

```
ssl_enable=YES
rsa_cert_file=/etc/ssl/certs/vsftpd.crt
rsa_private_key_file=/etc/ssl/private/vsftpd.key
```

Existeixen altres directives relacionades amb TLS però no són obligatòries especificar-les (com ara: 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, ...

Si volguéssim fer servir els usuaris emmagatzemats en una base de dades MySQL, caldria fer el següent:

1.- Comprovar de tenir instal·lat el mòdul libpam-mysql (ó pam_mysql en Fedora)

2.- Crear una base de dades (anomenada "vsbd", per exemple) amb una taula d'usuaris (anomenada "usuarios", per exemple) amb els camps: *id*, *nom*, *contrasenya*, *estat* ; i una altra taula (anomenada "bitacora", per exemple) amb els camps: *missatge*, *usuari*, *procés* (de tipus int), *servidor*, *client*, *moment* (de tipus timestamp).

3.- Crear dos usuaris MySQL: un que només llegeixi de la taula usuaris i escrigui a la taula d'intents (anomenat "userdb", per exemple), i un altra amb privilegis d'administració a la base de dades.

4.- Modificar el PAM (/etc/pam.d/vsftpd): primero, para que no se exija la existencia de los usuarios en el sistema operativo, desactivamos "pam_ftp.so", "common-account", "common-auth" y "pam_shells.so" añadiendo el símbolo "#" al inicio de cada línea donde aparezcan. Seguidamente, hay que añadir lo siguiente.

```
auth required pam_mysql.so verbose=0 user=userdb passwd=contraseña1 host=localhost
db=vsbd table=usuarios usercolumn=nom passwdcolumn=contrasenya statcolumn=estat crypt=2
sqllog=true logtable=bitacora logmsgcolumn=missatge logusercolumn=usuari logpidcolumn=proces
loghostcolumn=client logtimecolumn=moment
```

```
account required pam_mysql.so verbose=0 user=userdb passwd=contraseña1 host=localhost
db=vsbd table=usuarios usercolumn=nom passwdcolumn=contrasenya statcolumn=estat crypt=2
sqllog=true logtable=bitacora logmsgcolumn=missatge logusercolumn=usuari logpidcolumn=proces
```

loghostcolumn=client logtimecolumn=moment

(donde “contraseña1” de las líneas debe ser la misma que hemos fijado para el usuario "userdb")

5.-Al fitxer vsftpd.conf hem de tenir la següent directiva: *pam_service_name=vsftpd* (per defecte ja hi és, però per assegurar-se)

6.-Crear un usuari del sistema al qual es mapejaren tots els usuaris de la BD (amb les directives *guest_enable=YES* i *guest_username=usuariSistema*) per tal d’aplicar-li els permisos adients

7.-Opcional. Acabar de configurar el servidor VsFtpd , amb *user_config_dir* i demés, si es vol

Si hi ha problemes, es pot consultar el registre de VsFtpd (/var/log/vsftpd.log) ó de Pam (/var/log/auth.log) ó de MySql (/var/log/mysql.log i mysql.err)

Clients FTP

El client FTP clàssic ja ve instal·lat de forma predeterminada en un sistema Ubuntu. Es pot executar o bé escrivint *ftp* (indicant llavors a posterior, en el shell propi on s’hi entra, el servidor amb qui es connectarà) o bé escrivint *ftp ip.Serv.Ftp*

La llista de comandes més importants són

open ip.Serv.Ftp : per connectar amb un servidor FTP un cop dins del shell propi del client
user nomUsuari : per indicar l'usuari que es farà servir. La contrasenya es pregunta interactivament
ls , *pwd* , *cd* , *mkdir* , *rmdir* : comandes homònimes a Linux que s'executaran al servidor remot
!ls , *!pwd* , *!cd* ... : comandes homònimes a Linux que s'executaran a l'ordinador local
mput nomFitxer : puja els fitxers indicats de carpeta actual local a carpeta actual remota (accepta *?)
mget nomFitxer : baixa els fitxers indicats de carpeta actual remota a carpeta actual local (accepta *?)
mdelete nomFitxer : elimina els fitxers indicats de la carpeta remota (accepta *?)
close : tanca sessió
quit o *bye* : tanca sessió i surt del shell interactiu

Un altre client FTP és Ncftp (<https://www.ncftp.com>), el qual té la particularitat d'estar basat en Ncurses. Desgraciadament, cap d'aquests clients suporta connectivitat basada en TLS. Un client que sí que la suporta és Lftp (<https://lftp.yar.ru>), el qual es pot executar des del terminal així: *lftp -u usuari ip.Serv.Ftp* Les comandes disponibles dins del seu shell interactiu són similars a la ja conegudes: destacar que *mdelete* se substitueix per *mrm*, *quit* per *exit* i que hi ha més comandes, com ara *cat nomFitxer* (remot), *more nomFitxer* (remot), *mirror -v carpeta* (per baixar recursivament tot) o *mirror -R carpeta* (per pujar recursivament tot), entre altres

NOTA: Per a què Lftp suporti certificats autosignats (per defecte els rebutja) cal especificar la següent línia: *set ssl:verify-certificate no* , ja sigui directament dins del seu shell interactiu (llavors el "suport" durarà fins que es tanqui la sessió actual) o bé dins de l'arxiu de configuració ~/.lftp/rc (propi per un usuari particular) o /etc/lftp.conf (general per tothom)

També disposem de Filezilla (<https://filezilla-project.org>) el qual és un client plenament gràfic (i també suporta TLS anant a l'opció "New Site --> FTP over TLS)