

Apuntes de FTP y VSFTPD

Índice

1. [Introducción a FTP](#)
2. [Modos de Transferencia: Activo y Pasivo](#)
3. [Instalación y Funcionamiento de VSFTPD](#)
4. [Configuración General de VSFTPD](#)
5. [Forzar Modo Activo o Pasivo](#)
6. [Usuarios Anónimos](#)
7. [Enjaular \(Chroot\) Usuarios FTP](#)
8. [Excepciones a la Cárcel \(chroot_list\)](#)
9. [Userdir + Apache + FTP](#)
10. [Conexión Gráfica con FileZilla](#)
11. [Conexión Segura con SFTP](#)
12. [Enjaular Usuarios SFTP con SSH](#)
13. [Enlaces de Interés](#)

1. Introducción a FTP

FTP (**File Transfer Protocol**) es uno de los protocolos más antiguos para transferir ficheros entre un cliente y un servidor.

Características principales:

- **No es seguro:** el usuario y la contraseña viajan en texto plano.
- Usa **dos canales**:
 - Canal **de control** (comandos)
 - Canal **de datos** (transferencias)
- Funciona en **modo activo** o **modo pasivo**

Se usa habitualmente para:

- ✓ Servidores web
- ✓ Servidores internos
- ✓ Acceso rápido a carpetas de usuario

2. Modos de Transferencia: Activo y Pasivo

Modo Activo (PORT)

- Cliente se conecta al servidor por **21 (control)**
- El servidor abre una conexión de datos desde **el puerto 20** hacia un puerto aleatorio del cliente

- Si el cliente está detrás de un firewall → **suele fallar**

Ejemplo:

```
ftp> get file1
local: file1 remote: file1
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for file1 (0 bytes).
0 0.00 KiB/s
226 Transfer complete.
ftp> !ls | grep file1
file1
```

● Modo Pasivo (PASV)

- Cliente se conecta al servidor por **21**
- El servidor le responde con un puerto aleatorio (>1024)
- Es el modo recomendado.

Ejemplo:

```
ftp> get file1
local: file1 remote: file1
229 Entering Extended Passive Mode (|||13459|)
150 Opening BINARY mode data connection for file1 (0 bytes).
0 0.00 KiB/s
226 Transfer complete.
ftp> !ls | grep file1
file1
ftp>
```

3. Instalación y Funcionamiento de VSFTPD

```
sudo apt install vsftpd
sudo systemctl enable --now vsftpd
sudo systemctl status vsftpd
```

Puertos típicos:

- **21** → Control
- **20** → Datos en modo activo
- **>1024** → Datos en modo pasivo

Descarga y subida de archivos:

get <nombre/ruta-archivo> --> Coge un archivo del servidor y lo descarga en el cliente.

put <nombre/ruta-archivo> --> Envía un archivo desde el cliente hasta el servidor.

Entorno de los comandos:

Otro aspecto a tener en cuenta cuando utilizamos FTP es el entorno de los comandos, depende de como se escriban se ejecutaran en el lado del servidor o del cliente:

- `!ls` --> Esto se ejecuta en el cliente.
- `ls` --> Esto se ejecuta en el servidor.

Con el carácter `!` podemos ejecutar comandos en el cliente mientras estamos conectados por FTP.

Excepción:

Esto no aplica para los comandos `get` y `put`.

4. Configuración General de VSFTPD

Archivo principal:

```
/etc/vsftpd.conf
```

Parámetros básicos:

```
listen=YES/NO
listen_ipv6=YES/NO
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
```

Después de modificar:

```
sudo systemctl reload vsftpd
```

5. Forzar Modo Activo o Pasivo



Forzar modo activo

```
pasv_enable=NO
port_enable=YES
```



Forzar modo pasivo (recomendado)

```
pasv_enable=YES  
pasv_min_port=10000  
pasv_max_port=10050
```

Al configurar el modo pasivo podemos limitar los puertos que se utilizan, la única condición es que todos estén por encima del puerto 1024.

6. Usuarios Anónimos

Habilitar acceso anónimo

```
anonymous_enable=YES → Habilitem l'accés al servidor per a usuaris anònims.  
write_enable=YES → Donem permisos d'escriptura, si no no deixa pujar  
fitxers.  
anon_mkdir_write_enable=NO → No li donem permisos per crear directoris.  
anon_upload_enable=YES → Li donem permisos per pujar fitxers.
```

La raíz por defecto del usuario anonymous es **/srv/ftp**.

Para permitir subir archivos sin comprometer la seguridad:

```
sudo mkdir /srv/ftp/upload  
sudo chmod 777 /srv/ftp/upload
```

También puedes cambiar la home del usuario anónimo:

```
anon_root=/srv/ftp/public
```

Aspecto importante:

El propietario de la raíz del usuario anónimo por defecto es **root**, se puede cambiar con directivas pero es un agujero de seguridad, por lo tanto, si queremos que se puedan subir archivos a la raíz del usuario anónimo lo mejor es crear un directorio como hemos visto anteriormente.

7. Enjaular usuarios FTP

“Enjaular” significa que un usuario **no puede salir de su /home** y la ve como si fuera **/**.

```
chroot_local_user=YES
```

Ejemplo:

```
aaroncanofdez@aaron-cano-disk:~$ ftp 10.59.212.45
Connected to 10.59.212.45.
220 (vsFTPD 3.0.5)
Name (10.59.212.45:aaroncanofdez): roma
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
Remote directory: /
ftp> ls
229 Entering Extended Passive Mode (|||10021|)
150 Here comes the directory listing.
-rw-r--r--  1 1001  1001      6 Nov 23 16:35 hello.txt
226 Directory send OK.
ftp>
```

Problema habitual:

El directorio home no puede ser escribible por seguridad, así que se debe crear una subcarpeta para subir archivos.

8. Excepciones a la jaula (chroot_list)

Crear archivo (o editar si ya existe o ya se ha creado previamente):

```
/etc/vsftpd.chroot_list
```

Configurar:

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

Los usuarios listados en este archivo **NO estarán enjaulados**.

Ejemplo:

```
aaron
```

Solo deben añadirse los nombres de los usuarios que no se quieren enjaular, no hayq que especificar nada más.

9. Userdir + Apache + FTP

Permite que cada usuario tenga su propia web:

```
/home/usuario/public_html
```

Activar el módulo:

```
sudo a2enmod userdir  
sudo systemctl reload apache2
```

Crear archivo `index.html` y subirlo:

```
<h1>Bienvenido a user dir</h1>
```

```
ftp> put index.html
```

URL de acceso:

```
http://host/~usuario
```

10. Conexión Gráfica con FileZilla

FileZilla es un cliente de FTP que nos permite manejar el protocolo con una interfaz gráfica.

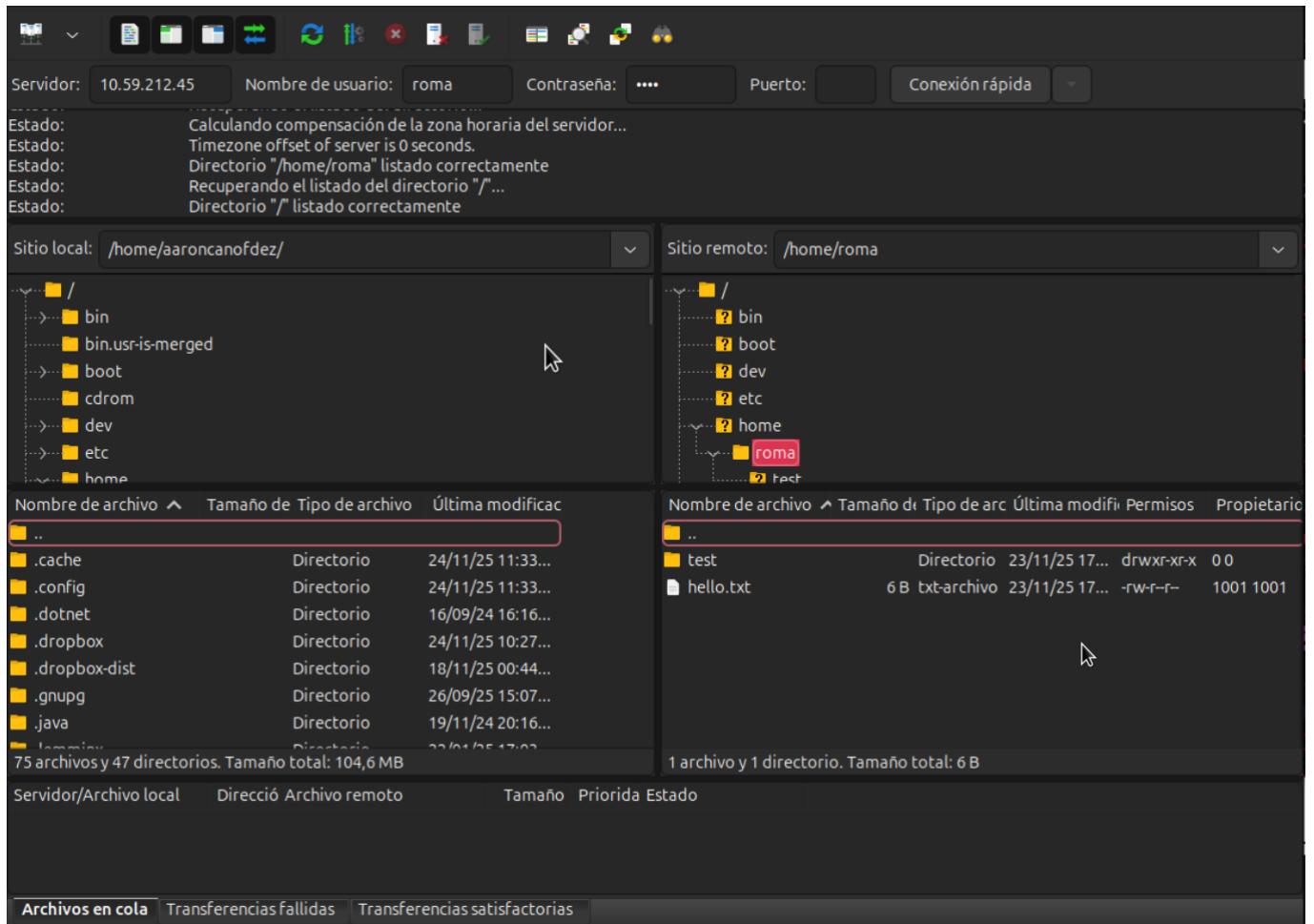
Para utilizarlo tenemos que instalarlo en la máquina cliente:

```
sudo apt install filezilla
```

Cuando abramos FileZilla veremos los siguientes campos para conectarnos con el servidor:

- Servidor (IP del servidor a conectarnos)
- Nombre de usuario (Nombre de usuario existente en el servidor)
- Contraseña (Contraseña del usuario)
- Puerto (Puedes especificar un puerto si lo deseas, por defecto usa el 21 y para SFTP puedes utilizar el 22).

Ejemplo de conexión con FileZilla:



En este caso nos hemos conectado con un usuario que no está enjaulado, por eso podemos ver todo el sistema de archivos del servidor.

11. Conexión Segura con SFTP

```
sftp usuario@servidor
```

Notas importantes:

- **No usa FTP**, sino SSH.
- Todo el tráfico va cifrado.
- Si escaneamos la red con un sniffer (ej.: Wireshark) lo identifica como SSH, no como FTP.

12. Enjaular Usuarios SFTP con SSH

Editar `/etc/ssh/sshd_config`:

```
Match User nombreusuario
    ChrootDirectory /home/nombreusuario
    ForceCommand internal-sftp
    X11Forwarding no
    AllowTcpForwarding no
```

Requisitos:

- El directorio raíz debe ser propiedad de root:

```
sudo chown root:root /home/nombreusuario
```

- Crear carpeta interior para subir archivos:

```
sudo mkdir /home/nombreusuario/upload
sudo chown nombreusuario:nombreusuario /home/nombreusuario/upload
sudo chmod 755 /home/nombreusuario/upload
```

Reiniciar SSH:

```
sudo systemctl reload sshd
```

13. Enlaces de Interés

- Directivas VSFTPD http://vsftpd.beasts.org/vsftpd_conf.html
- Administración de usuarios y grupos
http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m1/administracin_de_usuarios_y_grupos.html
- Userdir en Apache <https://www.evaristogz.com/configurar-userdir-automatico-apache2/>

Hecho por Aarón Cano ([rxnwashere](#))