

FTP

FTP (File Transfer Protocol) es un protocolo de red utilizado para la **transferencia de archivos** entre sistemas conectados a una red TCP/IP. Fue desarrollado en la década de 1970 y es ampliamente utilizado para el intercambio de archivos en entornos de red.

FTP permite a un cliente FTP conectarse a un servidor FTP para realizar operaciones de transferencia de archivos. Estas operaciones incluyen la **descarga** (transferencia desde el servidor al cliente) y la **carga** (transferencia desde el cliente al servidor) de archivos.

1. Instalación y configuración por defecto del servidor vsftpd

Tipos de conexiones FTP

Se puede conectar a un servidor FTP de 3 formas diferentes:

- Desde una terminal de Linux o Windows mediante comandos
- Desde un cliente FTP como FileZilla o gFTP.
- Desde un navegador (chrome, Firefox)

Conexión por navegador a un servidor FTP

Para conectar a un servidor FTP desde un navegador, deberemos especificar el protocolo, puesto que de no hacerlo el navegador entiende que queremos conectar por HTTP. Por lo tanto, el formato sería:

```
ftp://IPdelServidor
```

Podemos por ejemplo conectar al FTP de Rediris (<ftp://ftp.rediris.es/>) para encontrar distribuciones de Linux. Busca y descarga las ISO de las últimas versiones de Ubuntu. Una vez comience la descarga, cancelarla para no saturar la red.

El nombre de dominio no tiene por qué llevar ftp delante, pero es el subdominio que se suele utilizar para diferenciarlo del dominio para el servidor web.

Instalar vsftpd {#instalar-vsftpd}

VSFTPD es un servidor FTP para Linux. Soporta IPv6 y SSL, por lo que también permite conexiones FTPS. Es el servidor FTP por defecto en muchas distribuciones Linux, como por ejemplo Ubuntu.

Instalar el servidor FTP, realizando previamente un update para actualizar la información desde los repositorios. Necesitaremos permisos de administrador para ello:

```
foo@bar:~$ sudo apt update
foo@bar:~$ sudo apt install vsftpd
```

Comprobar creación de usuario y grupo FTP {#comprobar-creación-de-usuario-y-grupo-ftp}

Comprobar que se han creado un usuario y un grupo ftp. Para ello consultar los dos archivos y buscar el grupo y usuario creados:

```
foo@bar:~$ cat /etc/passwd
foo@bar:~$ cat /etc/group
```

Apertura de conexión {#apertura-de-conexión}

Comprobar que el servidor está iniciado y puerto de escucha. Podemos comprobar que el demonio vsftpd está escuchando en todas las interfaces de red en el puerto 21

```
foo@bar:~$ sudo netstat -plunt | grep ftp
```


El 21 es el puerto FTP para enviar y recibir comandos. Cuando se inicie la transferencia de archivos, veremos que se abre también otro puerto para transferir los datos.

Carpeta de almacenamiento {#carpeta-de-almacenamiento}

Comprobar que se crea la carpeta /srv/ftp. Por defecto, los archivos a servir mediante el servidor FTP se alojarán en esta carpeta, aunque esto se puede modificar. Podemos comprobar que esta carpeta existe y se encuentra vacía.

Archivo de configuración {#archivo-de-configuración}

Comprobar la creación y contenido del archivo /etc/vsftpd.conf, así como la configuración que trae por defecto.

 alt_text

Siempre es recomendable crear una copia de seguridad del archivo /etc/vsftpd.conf, por lo que guardaremos la copia con la extensión .bak (cualquier extensión es válida).

```
foo@bar:~$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
```

En el caso de que nuestro archivo de configuración quede inservible, tendremos una copia para restablecerlo.

Tipos de usuarios {#tipos-de-usuarios}

Vsftpd permite la conexión de diferentes tipos de usuarios:

- Usuarios ****anónimos**** (que ya hemos utilizado para hacer pruebas)

- Usuarios ****locales**** con cuenta en el sistema (/etc/passwd). Son los usuarios normales creados en nuestro servidor.
- Usuarios **virtuales**. Los usuarios virtuales son usuarios que no existen en el sistema (no figuran en /etc/passwd ni tienen un directorio home, ni se pueden loguear) pero sí pueden acceder a través del servidor FTP.

2. Conexión con usuario anónimo {#2-conexión-con-usuario-anónimo}

Creación de archivos en el servidor

Si se activa el acceso anónimo el directorio por defecto está en: /srv/ftp. Por defecto el servidor está configurado para que los usuarios anónimos sólo puedan descargarse ficheros de ese directorio.

Crearemos archivos de texto para hacer pruebas en /srv/ftp. Cambia los nombres por tus preferencias personales.

- plato.txt (lasaña.txt si es tu plato preferido)
- pelicula.txt
- grupodemusica.txt

Podemos crear todos los documentos con ****sudo touch**** si los queremos crear vacíos.

Conectar al servidor

Iniciar sesión en desktop y conectar al servidor FTP abriendo un terminal y utilizando el cliente FTP por comandos, o bien desde la máquina anfitrión Windows, si tenemos conectividad IP:

- ftp IPdelServidor
- ftp ftp.dmoreno.smx2.org (si disponemos de servidor DNS configurado)

Por defecto existe un usuario anónimo creado en el servidor que puede ser utilizado para conectarse a él. Las credenciales son:

- name: anonymous
- password: (vacío)

Si todo es correcto nos dará un Login successful (código 230). Veremos que no nos deja, de momento.

Permitir acceso anónimo {#permitir-acceso-anónimo}

Podemos consultar en el archivo de configuración si está permitido el acceso con usuario anónimo mirando la directiva el valor de la directiva **anonymous_enable**.

Por defecto viene deshabilitado, por lo que tendremos que cambiar el parámetro a YES. De este modo, permite únicamente conexión y descarga de archivos.



Reiniciamos el servidor y volvemos a comprobar desde un cliente que podemos acceder al servidor con el usuario anónimo.

Descargar archivos

Para listar el contenido de una carpeta puede utilizar ls. El contenido que tendríamos que ver al entrar es el de la carpeta /srv/ftp. Nos podemos mover por las carpetas como en una shell normal de linux, siempre que tengamos acceso y permisos para ello.

Con ls y cd nos vamos moviendo por las carpetas remotas.

Utilizando el comando **get** de ftp podemos probar a descargar un archivo del servidor. El archivo que le pasemos como argumento se descargará en la carpeta local en la que nos encontremos del cliente. Por ejemplo:

```
FTP> get pelicula.mp4
```

Conéctate y descárgate un archivo del servidor de un compañero

También podemos descargar varios archivos al mismo tiempo con la orden **mget** archivo especificado una expresión regular. Por ejemplo: *.pdf, descargará todos los archivos con extensión pdf.

Subir archivos

Intenta subir un archivo que tengas en una carpeta del cliente al servidor, utilizando:

```
FTP> put archivo.doc
```

Los usuarios anónimos no tienen permisos para subir archivos. Para ello deberemos cambiar varias directivas:

1. La directiva principal es **anon_upload_enable**. Si queremos que el usuario anónimo pueda subir archivos, lo cambiamos a **YES**.
2. También necesitaremos poder escribir en la carpeta, por lo que debemos cambiar **WRITE_ENABLE=YES**.
3. Crearemos una carpeta dentro de **/srv/ftp** llamada **uploads** que utilizaremos para poder subir archivos.
4. A esta carpeta uploads le haremos
 1. Cambio de propietario: `sudo chown ftp:ftp /srv/ftp/uploads`
 2. Cambio de permisos: `sudo chmod 757 /srv/ftp/uploads`

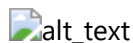
Enjaulado de usuarios {#enjaulado-de-usuarios}

Si no configuremos correctamente el servidor, podríamos permitir a un usuario cualquiera que navegara por todas las carpetas del sistema a su aire, con los problemas de seguridad que esto conlleva.

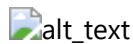
El usuario anónimo está enjaulado (**chrooted**), por lo que no puede salir del directorio asignado por defecto. Un usuario enjaulado solo puede acceder a una carpeta determinada, y no puede acceder a nada fuera de ella.

El usuario anónimo está enjaulado en **/srv/ftp**, por lo que no puede salir de esta carpeta. Podemos probar de movernos a otra la carpeta, como por ejemplo /home. Veremos cómo no nos deja acceder.

Ojo: el usuario no verá nada fuera de su carpeta, y para él la carpeta base será su raíz. Es decir: el en lugar de ver que está en /srv/ftp (ubicación real en el servidor) verá /. Del mismo modo, cuando esté en /srv/ftp/hola/que/tal.txt él verá la ruta /hola/que/tal.txt



Vemos que no nos permite cambiar de directorio. Salimos de la consola FTP con el comando **bye**. También se puede utilizar el comando **quit**.



3. Usuarios locales {#3-usuarios-locales}

Crear usuarios locales {#crear-usuarios-locales}

Para esta práctica vamos a crear varios usuarios locales para poder utilizarlos en el servidor FTP. Cada usuario tendrá su propia carpeta en home.

Crearemos contenido para 2 de los usuarios:

- Profesor
- Alumno

La contraseña será pa\$\$w0rd. Para crear los usuarios: sudo adduser XXX. Tras crear los usuarios, intentar acceder por FTP con estos.

Configurar espacio alumno {#configurar-espacio-alumno}

En primer lugar, iniciaremos sesión en el servidor como ****alumno**** y crearemos en su home las siguientes carpetas y subcarpetas en su home

- Apuntes
 - sox
 - sx
 - seg
 - eie
 - aw
- Trabajos
- ISOs
- Programas

Comprueba accediendo desde el navegador del cliente que se han creado las carpetas correctamente.

Carpetas del usuario profesor {#carpetas-del-usuario-profesor}

Iniciar sesión como ****profesor**** y crear las siguientes carpetas en su carpeta personal

- Exámenes
- Tutoría
- Reuniones

Comprueba accediendo desde el navegador del cliente que se han creado las carpetas correctamente.

Esto dos usuarios no pueden ejecutar comandos con privilegios de administrador, por lo que volvemos a cambiar al usuario principal, puesto que estos usuarios no son **sudoers**.

Habilitar login con usuarios locales {#habilitar-login-con-usuarios-locales}

No siempre nos estará permitido conectar al servidor FTP utilizando usuarios locales del servidor. En `/etc/vsftpd.conf`, habilitar la conexión de usuarios locales mediante el parámetro:

Local enable=YES

Prueba a colocarlo en NO y vuelve a probar de acceder al servidor FTP.

Al final, lo volvemos a dejar en YES y deshabilitamos el usuario anónimo (mirar arriba cuál era el parámetro)

Acceder al FTP con otros usuarios {#acceder-al-ftp-con-otros-usuarios}

En los siguientes puntos conectaremos como los otros usuarios locales y veremos cómo cada uno de ellos accede a su home. Si todo es correcto, podremos ver el contenido de la carpeta home de cada usuario. Por ejemplo, el usuario profesores accede al conectarse por FTP a su carpeta personal, **/home/profesores**.

Conéctate al servidor un compañero por consola

Conectar por consola a un servidor FTP

Para acceder con un usuario, desde una máquina cliente abrir un terminal (shell) de Linux o en el intérprete de comandos de Windows (cmd) y ejecutar:

- `ftp IPdelServidor` (cambiando por la dirección de vuestro servidor).
- Nos preguntará usuario y password que le diéramos a este usuario
- Si todo es correcto, nos situará en la carpeta home del usuario.
- Veremos que el prompt cambia por **FTP>**

Navegar por las carpetas del servidor

Una vez conectados, podemos ejecutar diferentes comandos, como por ejemplo `ls` para listar el contenido de la carpeta remota. Si el servidor está en una máquina Windows, los comandos deberán ser los de Windows (dir, por ejemplo).

También podremos ver el contenido de la carpeta de nuestra máquina cliente. Con `!ls` podemos mostrar el contenido de la carpeta local si se trata de un cliente Linux. En general, todos los comandos con `!` delante se ejecutan en el cliente.

En caso de Windows, los comandos suelen empezar con `L` (`ldir`, `lcd`, etc.)

Cambiar de servidor

Desde el mismo prompt **FTP>**, **nos podemos desconectar de un servidor y conectando a otro utilizando la orden **disconnect**. Para conectar a otro servidor FTP, dentro del prompt lo haremos con **open** `IPdeOtroServidor`. **De este modo podemos ir entrando y saliendo de diferentes servidores.

Cambiar de usuario dentro del servidor

Dentro del mismo servidor, podemos cambiar de usuario con la orden **user**, sin salir de él.

Consultar el fichero de log {#consultar-el-fichero-de-log}

Podemos consultar el archivo de log para comprobar cuáles han sido los últimos acontecimientos. En principio el log se guarda en **/var/log/vsftpd.log**. Lo podemos visualizar:

```
foo@bar:~$ sudo cat /var/log/vsftpd.log
```

Vemos que ha ido registrando todas las acciones que hemos realizado hasta el momento. Igualmente a al hacerse el archivo más grande es recomendable filtrar con **grep** o utilizar **tail** para visualizar solamente una parte del log.

Si queremos tener más detalle en el log, podemos configurar en **/etc/vsftpd.conf**:

```
log_ftp_protocol=YES
xferlog_enable=YES
xferlog_std_format=NO
```

Monitoriza tu log con **tail -f /var/log/vsftpd.log** y mientras se está ejecutando, pide conectarse a un compañero a tu servidor para ver lo que hace en tiempo real

Habilitar subida de archivos locales {#habilitar-subida-de-archivos-locales}

Intentamos subir con ambos usuarios un archivo al servidor utilizando el comando **PUT**. Veremos que no nos deja.

```
FTP> put hola.txt
```

El archivo tiene que existir en la carpeta local en la que estamos en ese momento.

Intentar ver contenido fuera de su carpeta: por ejemplo **/home**. Veremos que este usuario no está enjaulado, y por tanto puede ver cualquier contenido de cualquier carpeta.

Modificar el archivo de configuración del servidor FTP, y:

1. Permitir que los usuarios locales puedan subir archivos al servidor mediante el parámetro: **write_enable=YES**
2. Es probable que también sea necesario agregar la directiva **allow_writeable_chroot=YES** para poder subir archivos.

Reiniciar el servidor para aplicar cambios

Pídele a un compañero que se conecte a tu servidor y te suba un archivo. Conéctate tú al suyo y haz lo mismo.

Descarga un archivo fuera de la carpeta del usuario

Conecta como profesor y prueba a descargar el archivo del servidor **/etc/passwd**. Verás que lo puedes descargar, estando este archivo fuera de tu home. Como comprenderás, esto no es una buena idea por razones de seguridad.

Conviene que los usuarios solo se descarguen cosas de su propia carpeta home. En el siguiente paso intentaremos arreglarlo.

Enjaular usuarios locales {#enjaular-usuarios-locales}

Modificar **/etc/vsftpd.conf** y habilitar que usuarios locales sean “enjaulados” en su directorio home:

chroot_local_user=YES. De esta forma, no podrán acceder a ninguna carpeta fuera de su home (recomendable por temas de seguridad).

Reiniciar el servidor para aplicar cambios

Comprobar poniendo la variable a YES y NO, si podéis o no acceder a otro lugar fuera de la carpeta personal. Consulta el fichero de log **/var/log/vsftpd.log** y comprobar que se han registrado los accesos y transferencias.

4. Configuración avanzada del servidor {#4-configuración-avanzada-del-servidor}

Activar mensaje de directorio {#activar-mensaje-de-directorio}

Activar el mensaje de directorio (**.message**). En este caso, nos servirá para presentar mensaje a los usuarios anónimos usando el archivo **.message** ubicado en el directorio **/srv/ftp**. Tendremos que crear este archivo que contendrá el mensaje a mostrar.

Configurar mensajes en los directorios {#configurar-mensajes-en-los-directorios}

Configurar un mensaje en el home de los dos usuarios (1 y 2) que diga:

```
“Este es el servidor de XXX. Bienvenido”
```

Con el siguiente comando redirigimos un texto hacia un archivo en concreto para crearlo y escribir en él lo que le digamos. Nos ahorramos tener que crear el archivo con un editor, escribir y salir de él.

El parámetro a incluir en la configuración es: **dirmessage_enable=YES**

Conéctate a un compañero para ver su mensaje de bienvenida y viceversa. Escribe en dos directorios un mensaje que explique qué se debe guardar en ese directorio.

Activar mensaje de bienvenida {#activar-mensaje-de-bienvenida}

También podemos hacer que aparezca un mensaje de bienvenida al conectar por FTP al servidor mediante la opción **ftpd_banner**, en el archivo de configuración del servidor: **/etc/vsftpd.conf**

Podemos modificarlo por lo que queramos. Por ejemplo:

```
ftpd_banner= "Bienvenido al servidor FTP de XXX."
```

Comprobación {#comprobación}

Conectar desde un shell al servidor FTP, y comprobar que aparecen los mensajes que hemos configurado previamente.

También podéis crear [banners ASCII art](#) para ponerlos en vuestros servidores, como curiosidad.

Configuración de tiempos de conexión {#configuración-de-tiempos-de-conexión}

Algunas opciones para configurar las conexiones

Podemos limitar a un tiempo máximo de conexión usuario para una descarga que se ha quedado estancada sin progresar utilizando el parámetro **data_connection_timeout=300** (5 minutos)

También es posible configurar el tiempo de espera para mantener establecidas conexiones inactivas (60sg): **idle_session_timeout=600**. Si se supera este tiempo conectado pero sin hacer nada, se termina la conexión.

Configura la sesión para que un usuario pueda estar como máximo 2 minutos conectado al servidor, y no pueda estar más de 30 segundos sin meter algún comando.

Configuración de número de conexiones {#configuración-de-número-de-conexiones}

Máximos clientes simultáneos conectados: **max_clients=5**. Solo 5 clientes podrán estar al mismo tiempo en el servidor. Al sexto cliente que quiera entrar al mismo tiempo, se le denegará el acceso.

También podemos limitar conexiones por IP: **max_per_ip =2**. No podrán conectarse más de 2 ordenador con la misma IP. Recordad que en caso de estar tras una NAT todos los ordenadores se ven desde fuera con la misma IP pública.

Configura que solo se puedan conectar 2 clientes como máximo y solo 1 por IP. Comprueba que funciona correctamente

Enjaular usuarios locales (chroot)

Enjaula a los usuarios locales dentro de su propio directorio personal, esta opción mejora la seguridad.

- Si el parámetro es **chroot_local_user=YES** se enjaula a todos los usuarios locales por defecto
- Si el parámetro es **chroot_local_user=NO** no se enjaula a ningún usuario local por defecto

Lista {#lista}

Se permite especificar una lista con los usuarios locales a los cuales se les enjaula mediante la directiva:

```
chroot_list_enable=YES
```

Especifica la ruta en donde se encuentra el archivo con la lista de usuarios enjaulados o no enjaulados. Se define por la directiva ****chroot_list_file=/etc/vsftpd.chroot_list.****El significado cambia en función de la directiva anterior:

- Si **chroot_local_user=NO**, entonces, indica la lista de usuarios enjaulados.
- Si **chroot_local_user=YES**, indicaría la lista de usuarios no enjaulados.

Enjaula a algún compañero

Limitar velocidad a los usuarios {#limitar-velocidad-a-los-usuarios}

Un usuario puede descargar archivos a la velocidad máxima que permita la conexión de subida del servidor FTP. Esto puede ser una buena idea, pero puede hacer que el servidor no pueda hacer nada más, u otros usuarios se vean limitados.

La siguiente directiva permite establecer el límite de la velocidad máxima transferencia de datos para los usuarios locales. En este caso 10 MB/seg.

```
local_max_rate=10485760
```

También podemos limitar la velocidad. En este caso, los usuarios anónimos usarán un ancho de banda de 1 MB/seg:

```
anon_max_rate=1048576
```

Probar a generar un archivo grande en el servidor y descargarlo desde el cliente para comprobar la velocidad que descarga que se obtiene. Para generar archivos de un tamaño: `truncate -s 200MB prueba200` (generará un archivo de 200 MB).

De mientras el compañero está descargando, visualiza con `netstat -plnt | grep vsftpd` qué puerto se está utilizando para la transmisión.

El compañero descarga de dos formas: desde el navegador primero y por consola después.

Limitar acceso a determinados usuarios {#limitar-acceso-a-determinados-usuarios}

Podemos denegar acceso al servidor a usuarios determinados, indicados en un archivo de configuración. Para habilitar esta opción:

```
userlist_enable=YES
```

La ruta del archivo con la lista de usuarios a los que se les deniega el acceso se especifica con el siguiente parámetro:

```
userlist_file=/etc/vsftpd.user_list
```

Deberemos crear este archivo y escribir en él los usuarios a los que queremos denegar el acceso. Una estrategia sería colocar los usuarios en este archivo y comentar o descomentar según sea necesario.

Mostrar archivos ocultos {#mostrar-archivos-ocultos}

Por defecto no se mostrarán los archivos que comiencen por un punto. Para mostrar los archivos ocultos y las carpetas . y .., podemos utilizar la siguiente opción, que resulta útil para no sobrescribir archivos ocultos.

```
force_dot_files = YES
```

Mostrar información de los archivos {#mostrar-información-de-los-archivos}

También puede resultar interesante esconder la información acerca del propietario de los archivos:

```
hide_ids = YES
```

5. Configuración separada para cada usuario local {#5-configuración-separada-para-cada-usuario-local}

Podemos crear un archivo con directivas para cada usuario por separado. Para ello, debemos especificar en primer lugar en el archivo de configuración la siguiente directiva>

```
user_config_dir = /etc/vsftpd/usuarios
```

Esta carpeta deberá existir, y por tanto habrá que crearla y añadir los permisos que sean necesarios para poder acceder a ella.

Dentro de la carpeta `**/etc/vsftpd/usuarios`, **deberemos crear un archivo de texto con el nombre del usuario que queremos configurar. Por ejemplo, pepe. Crearemos un archivo por cada usuario que queramos configurar.

Dentro de este archivo, la configuración se escribe igual que en `vsftpd.conf`. La única diferencia, es que lo que pongamos aquí afectará solo a pepe, y para él se ignorarán las directivas especificadas en el archivo general `vsftpd.conf`.

Por ejemplo, si queremos limitar a pepe, podríamos hacer lo siguiente:

```
echo "local_max_rate 1024" > /etc/vsftpd/usuarios/pepe
```

Un ejemplo de configuración podría ser:

```
local_root=/srv/ftp/pepe \  
dirlist_enable=YES \  
download_enable=YES \  
write_enable=YES
```

De este modo, la carpeta raíz para pepe sería ****/srv/ftp/pepe**** (que tendríamos que crear). Para el resto de usuarios, se aplicaría la configuración de `/etc/vsftpd`. Por lo tanto, ellos tendrían como raíz su `home`.

Crea un archivo de configuración para cada uno de tus compañeros de mesa y aplicarles diferentes opciones a cada uno.

6. Crear cuotas (no hacer nada a partir de aquí)

Los usuarios tienen por defecto espacio limitado en el servidor. Si esto no se controla, puede llegar un momento que un usuario ocupe todo el espacio libre del disco. Podemos limitar el espacio para un usuario concreto utilizando el paquete `quota`. Para instalarlo, ejecutando:

```
apt install quota
```

Agregar directiva a la partición {#agregar-directiva-a-la-partición}

En GNU/Linux antes de poder gestionarlas es necesario editar el fichero `/etc/fstab`, y añadir **usrquota** (cuota de usuario) o **grpquota** (cuota de grupo) como parámetro del punto de montaje del sistema de ficheros en el que queramos utilizar cuotas.

En `/etc/fstab` agregamos la directiva a la partición en donde queremos limitar la cuota: `Usrquota`

Añadirnos `usrquota`, `grpquota`, a la partición en la que queramos activar las cuotas de disco. Hacemos una copia de la línea (`++ctrl++K --- ++ctrl++U`) que vamos a editar, por si acaso, y la ponemos con comentarios.

```
/dev/hda1  /      ext3    **usrquota,grpquota**,errors=remount-ro 0      1
```

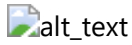
Reiniciar el sistema operativo

Comprobación

Chequeo del sistema de cuotas

Podremos chequear las cuotas en nuestro sistema con:

```
quotacheck -augmv
```



Comprobación de cuotas de usuarios {#comprobación-de-cuotas-de-usuarios}

Para listar las cuotas de los usuarios podemos utilizar `quota -u idusuario`

Para ver un informe de todas las cuotas:

```
repquota -a
```

Crear un usuario nuevo.

Reiniciar el sistema operativo y observar que en nuestro directorio de conexión se ha creado el fichero `aquota.user`

Limitar la cuota de cada usuario

Escribiendo el comando:

```
edquota "nombre de usuario"
```

7. Modos activo y pasivo (No hacer)

Utilizar cliente ftp para establecer conexión anónima con <ftp.rediris.es>.

Ejecutar el comando `ls`. Comprobar si deja o no

Utilizar el modo pasivo

Iniciar modo pasivo dentro de la consola FTP utilizando el comando `PASSIVE`

Ejecutar `LS` de nuevo

8. Configuración TLS/SSL/FTPS (No hacer)

Es recomendable utilizar este sistema para conectar desde Internet al servidor, puesto que las contraseñas, por ejemplo, se envían en texto plano. Para utilizar VSFTPD con encriptación (más seguro), se necesita modificar la configuración:

```
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
```

FTP utiliza el puerto 21 si no se especifica otra cosa. Para el protocolo **FTPS**, el puerto utilizado por defecto es el 990. Si se quiere cambiar, modificar: **listen_port=990**

Si tenemos instalado openssl no hace falta en principio crear ningún certificado.

Para probarlo necesitaremos, desde la consola de comandos ejecutar el mismo comando, pero cambiando ftp por ftps en la URL

```
ftp [ftps://IPdelServidor](https://IP)
```

9. Usuarios virtuales (NO HACER)

Instalar la librería PAM que nos ayudará a crear usuarios virtuales:

```
sudo apt install vsftpd libpam-pwdfile
```

Agregar las siguientes líneas al archivo de configuración si no existen actualmente.

```
listen=YES \
anonymous_enable=NO \
local_enable=YES \
write_enable=YES \
local_umask=022 \
nopriv_user=vsftpd \
virtual_use_local_privs=YES \
guest_enable=YES \
user_sub_token=$USER \
local_root=/var/www/$USER \
chroot_local_user=YES \
hide_ids=YES \
guest_username=vsftpd
```

Registramos los usuarios con **htpasswd**, con lo que se asume que Apache está ejecutándose en el servidor.

Creamos una carpeta para poner los archivos de configuración dentro

```
sudo mkdir /etc/vsftpd
```

Creamos el primer usuario:

```
sudo htpasswd -cd /etc/vsftpd/ftpd.passwd director
```

Para los siguientes usuarios:

```
sudo htpasswd -d /etc/vsftpd/ftpd.passwd user2
```

Hacer un backup de la configuración original de PAM

```
sudo mv /etc/pam.d/vsftpd /etc/pam.d/vsftpd.bak
```

Crear uno nuevo:

```
sudo vim /etc/pam.d/vsftpd
```

Copiar solo estas dos líneas:

```
auth required pam_pwdfile.so pwdfile /etc/vsftpd/ftpd.passwd \  
account required pam_permit.so
```

Crear un usuario local sin acceso a shell

```
sudo useradd --home /home/vsftpd --gid nogroup -m --shell /bin/false vsftpd
```

Reiniciar el servidor

Crear carpetas

- Carpeta raíz: /var/www/user1 con permisos 555
- Subcarpeta /var/www/user1/www con permisos 755
- Subcarpeta /var/www/user1/docs con permisos 755

Revisar que en vsftpd.conf tenemos chroot_local_user=YES para que el usuario no pueda ver nada fuera de esta carpeta.

```
mkdir /var/www/user1 \  
chmod -w /var/www/user1 \  
mkdir /var/www/user1/www \  

```

```
chmod -R 755 /var/www/user1/www \  
chown -R vsftpd:nogroup /var/www/user1
```

10. Clientes de ftp

Existen múltiples clientes para conectar por FTP. Entre ellos:

- WinSCP
- gFTP
- FlashFXP
- FileZilla