



2023  
2024



# Módulo: Despliegue de Aplicaciones Web



## Unidad de Trabajo: 2

Instalación y administración de servidores  
de transferencia de archivos



# Contenido de la unidad

<b>1</b>	<b><i>Introducción</i></b>	<b>3</b>
<b>2</b>	<b><i>Servicio de transferencia de archivos. Permisos y cuotas</i></b>	<b>3</b>
2.1	Permisos	3
2.2	Cuotas	4
2.3	Tipos de usuarios	5
2.4	Tipos de accesos al servicio	5
2.5	Tipos de transferencia de ficheros	5
<b>3</b>	<b><i>Modos de conexión</i></b>	<b>5</b>
3.1	Modo activo	6
3.2	Modo pasivo	6
<b>4</b>	<b><i>Instalación y configuración del servidor proFTPd en SO Linux</i></b>	<b>6</b>
<b>5</b>	<b><i>Utilización de herramientas gráficas y en modo texto (Comandos).</i></b>	<b>8</b>
5.1	Herramientas Gráficas	8
5.2	Uso del navegador	8
5.3	Uso de comandos	8
<b>6</b>	<b><i>Configuración y uso de cuotas</i></b>	<b>10</b>
6.1	Instalar y configurar las cuotas de disco	10
6.1.1	Instalar los paquetes necesarios.	10
6.1.2	Activar las cuotas en el sistema de archivos y volver a montarlo	11
6.1.3	Crear los archivos de cuota y la tabla de uso de espacio compartido	11
6.1.4	Configurar cuotas para usuarios y grupos	12
6.1.5	Establecer un valor para el periodo de gracia	13
6.2	Comprobar las cuotas de disco	13
6.3	Desactivar y volver a activar las cuotas.	14
<b>7</b>	<b><i>Protocolo seguro de transferencia de archivos</i></b>	<b>14</b>
<b>8</b>	<b><i>VirtualHosts en ProFTP</i></b>	<b>15</b>

## 1 Introducción

El **servicio de transferencia de ficheros** tiene un papel fundamental a la hora de desplegar una aplicación. Su función es transferir la información de desarrollo a producción en un entorno empresarial. Hoy en día estos problemas son fácilmente solucionables por parte de los hosting de Internet, que permiten acceder mediante aplicaciones FTP, como Filezilla, Cyberduck, o cualquier otra del mercado.

Además, también suelen permitir conexiones seguras implementando protocolos seguros como SSL, de hecho, **proFTPD** permite una implementación segura mediante certificados.

Para subir el código de las aplicaciones es necesario configurar el tiempo de conexión y el tamaño de los archivos para no colapsar ni el cliente ni el servidor. Hay que tener en cuenta que si el servidor web está en producción sería necesario controlar este aspecto o realizar una parada técnica para que los usuarios no sufran cortes innecesarios.

En el mundo tecnológico existen distintos servidores FTP. Para poder trabajar con ellos, se ha elegido la instalación y configuración de **proFTPD**, por ser uno de los más completos.

Existen varios modos de **conexión**, como son el **activo** y el **pasivo**, que van a depender de si existe un cortafuegos en mitad de la conexión o no.

Por otro lado, existen tres tipos de usuarios que se pueden habilitar en este tipo de servicio, como son **usuarios autenticados, virtuales y anónimos**.

En conclusión, es necesario que uses una aplicación segura para que no comprometa tu seguridad ni fuga de información con relación al código de tu aplicación.

## 2 Servicio de transferencia de archivos. Permisos y cuotas

El FTP, es un protocolo de red que permite la transferencia de archivos entre sistemas conectados entre sí. Se basa en la arquitectura cliente-servidor, de manera que desde un cliente existe la posibilidad de conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos, independientemente del sistema operativo.

La transferencia de archivos entre cliente – servidor puede ser de todo tipo, como por ejemplo imágenes, vídeos, texto, etc. La interfaz de transferencia puede ser mediante comandos o modo gráfico.

Aunque es uno de los métodos más usados en Internet, tiene un gran inconveniente, “la seguridad”. Por ello es muy importante configurarlo correctamente y tomar las medidas oportunas para evitar el acceso fraudulento de la información que se transfiere.

Como se ha comentado anteriormente, este servicio se basa en una arquitectura cliente-servidor, siendo el cliente quien solicita la conexión para transferir los archivos y el servidor es el que ofrece o almacena archivos dependiendo de la solicitud del cliente. Por lo tanto, es un servicio orientado a conexión que necesita establecer una conexión para poder transferir archivos.

Es **necesario** usar este servicio acompañado de algún **protocolo de seguridad**, como puede ser **SSL**, ya que de no hacerlo se corre el riesgo de que la información transferida sea hackeada por entidades externas.

El servidor de **FTP funciona a través de los siguientes puertos** configurables:

- **Puerto 21:** control de la conexión.
- **Puerto 20 o mayor de 2014:** puerto de transferencia de datos.

Hay que tener en cuenta que estos puertos son modificables mediante los archivos de configuración correspondientes. Pero si no se configura nada, por defecto, los puertos anteriores son utilizados por la arquitectura.

### 2.1 Permisos

Los **permisos** y las cuotas son una parte importante de la configuración del servicio FTP. Por ello es necesario controlar el espacio y los permisos de lectura y escritura de los usuarios que entran en el sistema desde el exterior. De no hacerlo así, podría aumentar el riesgo de amenaza desde el exterior y convertirse en riesgo real. Las amenazas podrían ser desde entrar en otro directorio que no sea el dedicado para el FTP, hasta que se caiga el sistema por falta de espacio.

Antes de entrar en detalle con las cuotas, se va a proceder a detallar cómo funcionan los permisos en Linux, para posteriormente explicar cómo asignar los permisos a un usuario.

Cuando se crea un fichero o carpeta en Linux, existen tres niveles de acceso que permiten controlar sus accesos, que son los siguientes:

- a) **Nivel propietario:** son los permisos que se asignan al propietario del archivo o directorio.
- b) **Nivel grupo:** son aquellos que se asignan a los grupos de usuarios. Esto es, un grupo puede tener de 1 a n usuarios.

- c) **Nivel usuarios:** este nivel corresponde a todos los usuarios definidos en el sistema operativo que no son los anteriores, o llamados “los otros”.

Los permisos en Linux son tres y se distinguen de la siguiente forma:

- 1) **Lectura (r):** el usuario podrá ver el contenido y visualizar un fichero o directorio. Si tiene asignado (-) no podrá visualizarlo.
- 2) **Escritura (w):** el usuario podrá modificar el contenido del archivo o directorio.
- 3) **Ejecución (x):** el usuario podrá ejecutar el archivo.

Podremos aplicar permisos para cada uno de los niveles anteriores (propietario, grupo y otros). Usando el comando de Linux “ls -l”, podremos ver los permisos anteriormente explicados para cada uno de los niveles.

```
usuario@vbox:~$ ls -l
total 32
drwxr-xr-x 2 usuario usuario 4096 ene 7 13:10 Descargas
drwxr-xr-x 2 usuario usuario 4096 ene 7 13:10 Documentos
drwxr-xr-x 2 usuario usuario 4096 ene 7 13:10 Escritorio
drwxr-xr-x 2 usuario usuario 4096 ene 7 13:10 Imágenes
drwxr-xr-x 2 usuario usuario 4096 ene 7 13:10 Música
drwxr-xr-x 2 usuario usuario 4096 ene 7 13:10 Plantillas
-rw-rw-r-- 1 usuario usuario 0 ene 7 13:12 prueba.txt
drwxr-xr-x 2 usuario usuario 4096 ene 7 13:10 Público
drwxr-xr-x 2 usuario usuario 4096 ene 7 13:10 Vídeos
usuario@vbox:~$
```

Para asignar permisos en Linux se usan los siguientes comandos:

- **chmod:** este comando puede modificar el permiso del propietario (u), los grupos (g) y los otros (o). Existen multitud de opciones para usar este comando, incluso se puede usar el sistema octal para aplicar permisos. La sintaxis general del comando es la siguiente:

chmod [opciones] modo-octal fichero.

- **chown:** permite cambiar el propietario del archivo o directorio. La estructura general del comando sería la siguiente:

chown [opciones] [usuario] [:grupo] fichero

## 2.2 Cuotas

Es posible establecer cuotas de espacio en disco tanto por usuario como por grupo para evitar que un determinado usuario o grupo monopolice el espacio en disco.

El espacio en disco es un recurso finito y una mala gestión de su uso puede provocar una denegación de servicio. Por ello será necesario controlar la actividad de los usuarios para evitar un mal uso del espacio en disco.

La cuota maneja los siguientes parámetros: el **soft limit**, el **hard limit** y el **periodo de gracia**

- Las **cuotas soft** establecen el umbral para avisar a los usuarios o grupos de que están llegando al límite máximo o cuota hard. Cuando se llega a esta cuota cada vez que un usuario que la ha sobrepasado escribe en el sistema de ficheros le aparece un mensaje en la terminal recordándoselo. Estas cuotas se pueden establecer por usuario o grupo.
- Las **cuotas hard** establecen la cantidad máxima de espacio que se puede utilizar y no se pueden sobrepasar a menos que el administrador las cambie. Estas cuotas se pueden establecer:
  - Por usuario. Una vez superado el usuario no podrá escribir en el sistema de ficheros.
  - Por grupo. Una vez superado, ningún usuario del grupo podrá escribir en el sistema de ficheros, a pesar de que no haya alcanzado su cuota como usuario.
- **Periodo de gracia:** Cuando se sobrepasa la cuota soft se entra en el periodo de gracia. Una vez terminado el periodo, no se le permitirá al usuario o grupo escribir en el sistema de ficheros hasta que libere el espacio necesario para estar por debajo de la cuota soft.  
Este periodo se puede especificar en meses, semanas, días, horas, minutos o segundos.

### Importante:

La cuota de disco permite establecer un límite máximo en el número de ficheros creados o el espacio ocupado por un usuario (cuota de usuario) o por el conjunto de usuarios que pertenecen a un grupo (cuota de grupo).

Para la gestión de la cuota, utilizaremos el programa “quota”

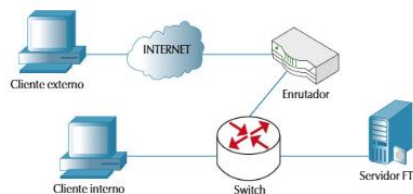
## 2.3 Tipos de usuarios

Existen tres grandes grupos de usuarios que se pueden conectar al servidor para almacenar o recuperar información, que se comentan a continuación:

- **Usuarios anónimos:** tienen acceso, pero los permisos están limitados por el sistema de archivos. Para conectarse al sistema usan una cuenta simbólica como **anonymous** y como password una cuenta de correo electrónico. Este tipo de usuario es un agujero de seguridad, por lo que es necesario tomar las medidas oportunas para evitar posibles accesos no deseados a la información.
- **Usuarios autenticados:** son aquellos que son propios del sistema operativo. Se requiere de un usuario y contraseña para entrar en el servidor FTP.
- **Usuarios virtuales:** se crean independientemente del sistema operativo con sus directorios home apropiados y creados para tal fin. Servidores como proFTPD poseen este tipo de usuarios que permiten no comprometer la seguridad del sistema, ya que no están creados en el mismo. La validación de estos usuarios no tiene por qué realizarla el sistema, sino que puede ser en un fichero de texto, una base de datos como Mysql o un servicio de directorio como LDAP.

## 2.4 Tipos de accesos al servicio

Con relación al acceso al servicio de FTP, se puede acceder de diferentes formas, ya sea desde una red local o desde Internet. A continuación, se pondrá un esquema de cómo acceder al servicio de FTP desde un cliente:



## 2.5 Tipos de transferencia de ficheros

A la hora de transferir archivos es necesario distinguir dos tipos de archivos para que la información que se traspase no sea inconsistente. Se comentan los tipos:

- **Archivos binarios:** son aquellos archivos que no son de texto y están codificados. Por ejemplo, serían los archivos tipo ejecutable, imágenes, archivos de audio y vídeo, etc. El comando para poder cambiar al tipo de fichero es `binary`.
- **Archivos de texto:** son ficheros de tipo ASCII, legibles totalmente, esto es, se puede interpretar la información fácilmente. Se representa el fichero ASCII mediante 7 dígitos binarios en base decimal para representar la información. Un ejemplo de este tipo de ficheros son los que terminan en `.txt`, `.xml`, `.html`, `.ps`, etc. En la transferencia ASCII, la transmisión se realiza analizando byte a byte la información transmitida. Los archivos ASCII terminan con un carácter de control EOF. Al usar una transferencia ASCII, en el momento que se recibe un byte que corresponde a EOF se da por terminada la transmisión. Esto para los archivos ASCII es lo que se debe producir, pero no para otros archivos ya que un byte de un fichero no ASCII puede contener el código correspondiente a EOF en cualquier parte del archivo. El comando para poder cambiar al tipo de fichero es `ascii`.

Es crucial saber de antemano qué ficheros se van a transferir, ya que, si no se usan las opciones adecuadas, se podría destruir la información. El servicio FTP permite configurar las opciones adecuadas en la transferencia de ficheros.

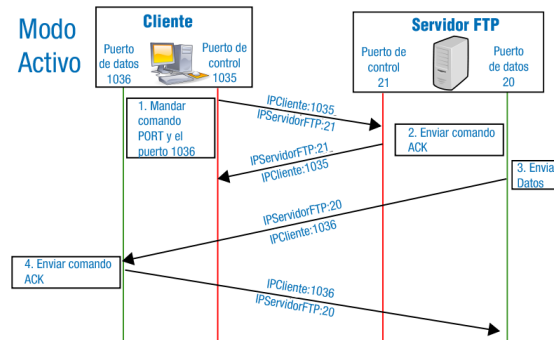
## 3 Modos de conexión

Cuando se realiza la comunicación entre el cliente y servidor existen dos modos de conexión por parte del cliente:

- Modo activo
- Modo pasivo

### 3.1 Modo activo

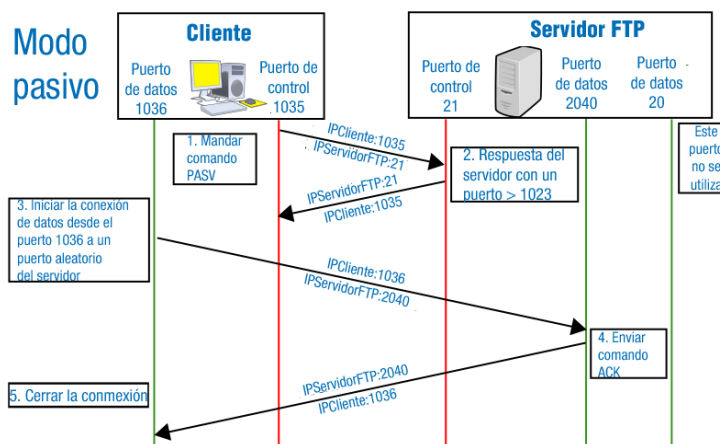
En el modo activo el servidor siempre crea un canal para datos por el puerto 20, mientras que el cliente asocia un puerto aleatorio mayor que 1021. El cliente envía un paquete al servidor, indicando el número de puerto para transferir archivos. Se puede observar en la siguiente figura el modo activo en funcionamiento:



### 3.2 Modo pasivo

Sin embargo, en modo pasivo, es el cliente quien comienza la conexión con el servidor para evitar bloqueos de conexión mediante configuraciones NAT o cortafuegos. En este modo, el cliente inicia ambas conexiones, control y datos. En este caso, el cliente envía un comando PASV sobre el canal de control (el puerto 21). El servidor FTP indica a través de este mismo canal el puerto del servidor al que debe conectarse el cliente (un puerto que será mayor a 1023 en el servidor). Entonces es el cliente quien inicia una conexión desde el puerto siguiente a su puerto de control hacia el puerto del servidor que se ha especificado anteriormente.

El diagrama de una conexión FTP en modo pasivo sería el siguiente:



**NOTA:** Antes de cada nueva transferencia, tanto en el modo Activo como en el Pasivo, el cliente debe enviar otra vez un comando de control y el servidor recibirá esa conexión de datos en un nuevo puerto aleatorio (si está en modo pasivo) o por el puerto 20 (si está en modo activo).

## 4 Instalación y configuración del servidor proFTPD en SO Linux

En este apartado vamos a ver el proceso a seguir para la instalación del **servicio proFTPD** para una distribución Linux (Debian).

La instalación se va a llevar a cabo en una máquina virtual, y posteriormente crearemos un **usuario virtual llamado admin** para que se pueda conectar al servidor FTP. La carpeta a la que accederá el nuevo usuario virtual **será /var/ftp/bbdd** (habrá que crearla)

#### Pasos para la instalación del servicio

- 1. Instalación del servicio proFTPD**

```
# apt update
# apt upgrade
# apt install proftpd
```
- 2. Crear el directorio al que se conectará el usuario del FTP:**

```
# mkdir -p /var/ftp/bbdd
```

3. **Detectar el uid del usuario ftp:** Antes de crear el usuario virtual, necesitamos saber cuál es el UID del usuario ftp (usuario con el que corre el servicio porFTPD)  
\$ id ftp

```
root@osboxes:/etc/proftpd# id ftp
uid=137(ftp) gid=65534(nogroup) grupos=65534(nogroup)
root@osboxes:/etc/proftpd#
```

4. **Crear usuario virtual:** una vez obtenido el uid del usuario ftp, podremos crear el nuevo usuario virtual (admin). Para la creación de un usuario virtual para el servicio proFTPD, necesitamos indicar:

- Nombre del usuario a crear**
- Directorio raíz:** Directorio al que se accederá una vez el usuario se valide
- UID del usuario ftp:** el identificador del usuario del sistema con el que corre el servicio
- Shell del nuevo usuario:** Como será un usuario virtual sólo para el servicio de FTP, no le asignaremos Shell del sistema
- Fichero de contraseñas:** Tendremos que indicar el fichero en el que se guardará el usuario nuevo a crear.

Una vez tengamos toda la información, crearemos el nuevo usuario con el siguiente comando:

```
# ftpasswd --passwd --name <<usuario_virtual>> --home <<directorio raíz para el nuevo usuario>> --uid <<UID del usuario FTP>> --shell /bin/false --file <<fichero de usuarios>>
```

```
root@osboxes:/etc/proftpd# ftpasswd --passwd --name admin --home /var/ftp/bbdd
--uid 137 --shell /bin/false --file /etc/proftpd/passwd.virtuales
ftpasswd: using alternate file: /etc/proftpd/passwd.virtuales
ftpasswd: --passwd: missing --gid argument: default gid set to uid
ftpasswd: updating passwd entry for user admin

ftpasswd: /bin/false is not among the valid system shells. Use of
ftpasswd: "RequireValidShell off" may be required, and the PAM
ftpasswd: module configuration may need to be adjusted.

Password:
Re-type password:

ftpasswd: entry updated
root@osboxes:/etc/proftpd#
```

5. **Propietario del directorio:** Se le debe cambiar el propietario de la carpeta a la que se va a conectar el usuario por FTP para que pertenezca al usuario con el que se ejecuta el servicio, es decir, usuario ftp  
# chown -R ftp /var/ftp/bbdd (-R es para que cambie el propietario recursivamente)
6. **Configurar el servicio:** El penúltimo paso que tendremos que realizar es la de configurar el servicio para permitir la conexión del usuario que hemos creado anteriormente. Para ello modificaremos dos directivas del fichero /etc/proftpd/proftpd.conf:
- AuthUserFile /etc/proftpd/passwd.virtuales** → Indicamos que tome del fichero passwd.virtuales, los usuarios que se pueden conectar por FTP
  - RequireValidShell off** → Indicamos que no debe de validar el usuario con el sistema operativo
7. **Reinicio del servicio:** El último paso, y más importante, es reiniciar el servicio de FTP para que se apliquen los cambios realizados  
# systemctl restart proftpd      # service proftpd restart



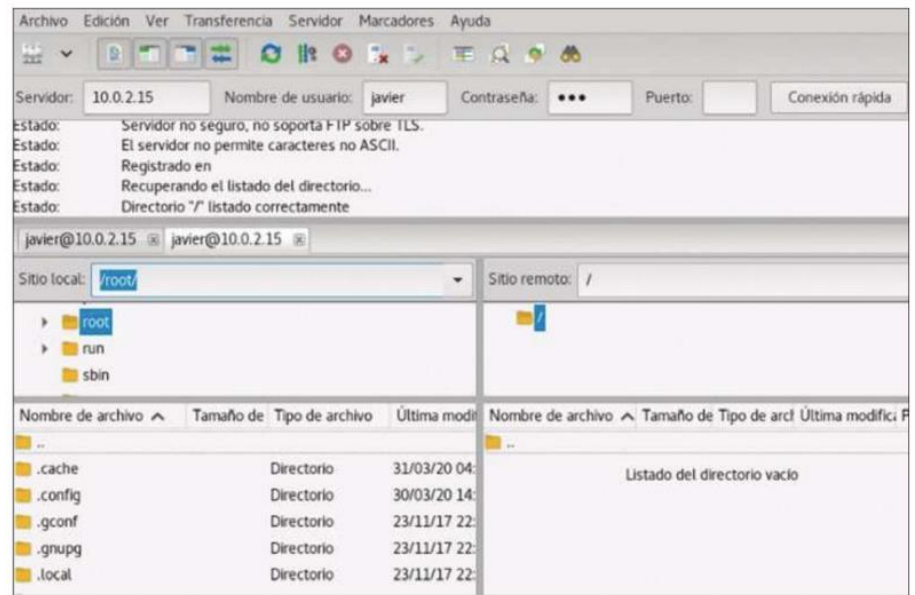
## 5 Utilización de herramientas gráficas y en modo texto (Comandos).

En este apartado se va a comentar uno de los interfaces gráficos más usados en el mundo de Internet y, más concretamente, a la hora de realizar transferencias de ficheros vía FTP. Posteriormente, se verán los comandos usados en la línea de comandos en la consola de FTP. Pero este método no es intuitivo ni práctico, por ello se usa una interfaz gráfica o el navegador.

### 5.1 Herramientas Gráficas

Todos los clientes de FTP de forma gráfica funcionan y se comportan del mismo modo. Normalmente poseen unos campos de entrada de datos típicos: la IP del servidor FTP remoto, usuario, contraseña y el puerto de conexión, que como se sabe, es configurable en el fichero de configuración del servicio FTP.

Por último, el interfaz tiene dos paneles, el panel de la izquierda es la máquina local y el panel de la derecha es el servidor remoto cuando se realiza la conexión. Por lo que el traspaso de información es tan fácil como arrastrar el fichero o directorios que se desee traspasar de un panel a otro, siempre teniendo en cuenta que se posea permiso para realizar la acción.



Uno de los **clientes FTP** gratuitos más usados es **Filezilla**. Este software es un cliente FTP Open Source rápido y capaz de manejar conexiones simultáneas. Soporta SFTP y FTPS. Además, está disponible para todos los sistemas operativos, Mac OS, Linux y Windows.

### 5.2 Uso del navegador

Hoy en día los navegadores que existen en el mercado usan normalmente el protocolo HTTP, pero la mayoría de los usuarios desconocen que tales navegadores tienen otro uso. Ese uso se refiere al empleo de otros protocolos, como pueden ser el FTP. Como se comentó anteriormente, se pueden usar herramientas diseñadas para ello, pero si se emplea el navegador se puede descargar información perfectamente.

Si se quiere usar el navegador como cliente FTP, solamente es necesario teclear en la barra de direcciones del navegador la siguiente línea:

```
ftp://nombre_servidor_ftp o dirección IP: puerto (por defecto el 21)
```

Supongamos que la IP del servidor es 192.168.1.20. En este caso, lo único que hay que hacer es teclear en la barra de direcciones del navegador `ftp://192.168.1.20`, no es necesario el puerto porque está configurado por defecto. En caso de que sea otro, sí es necesario teclearlo.

Si se teclean el usuario y la contraseña adecuada, se accederá a la carpeta correspondiente y configurada para ello en el servicio FTP.

El uso del navegador como cliente FTP no es muy funcional que digamos, ya que sólo sirve para descargar ficheros del servidor FTP. Por lo que para un uso puntual es efectivo, pero poco más.

### 5.3 Uso de comandos

También podemos conectarnos al servidor FTP haciendo uso de un cliente FTP mediante la terminal del sistema. Para ello deberemos tener el cliente FTP instalado.

En caso de no tenerlo instalado, usamos el comando

```
# apt install ftp
```

Una vez tengamos instalados el cliente FTP, podemos realizar la conexión al servidor FTP, usando la orden:

```
$ ftp <servidor>
```



Y posteriormente le indicamos el usuario y la contraseña del usuario con el que queremos conectarnos al servidor FTP

```

root@osboxes:/etc/proftpd# ftp localhost
Connected to localhost.
220 ProFTPD Server (Servidor FTP) [::1]
Name (localhost:root): admin
331 Contraseña necesaria para admin
Password:
230 Usuario admin conectado
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> !pwd
/etc/proftpd
ftp> pwd
257 "/" es el directorio corriente
ftp> !ls
blacklist.dat  ldap.conf  passwd.virtuales  prueba.txt  tls.conf
conf.d         modules.conf  proftpd.conf  sql.conf  usuario.ldif
dhparams.pem  ou.ldif     prueba         testdisk.log  virtuals.conf
ftp> ls
200 Comando EPRT exitoso
150 Abriendo ASCII modo conexión de datos para file list
-rw-r--r--  1 admin  pulse          20 Mar 30 17:20 prueba.txt
226 Transferencia completada
ftp>

```

Una vez conectado al servidor FTP, podemos observar el cambio del prompt del sistema, el cual nos indica que estamos conectados a un servidor FTP. A partir de ese momento podemos utilizar los comandos adecuados para poder realizar las acciones necesarias.

En esta sección se van a comentar los comandos más importantes que se usan en la consola de FTP y que permite realizar operaciones en el servidor. Se han agrupado en tres cuadros, el primero son **comandos para la conexión**, el segundo está relacionado con los **comandos para la gestión de los directorios** y el último con los **comandos para la gestión de ficheros**.

#### Comandos de conexión

Comando	Descripción
<b>open [IP]</b>	Abre una conexión con la IP que tecleemos.
<b>user [usuario]</b>	Solicita un usuario para autenticar.
<b>bye/exit/quit</b>	Se sale del interfaz de comandos de FTP, nos devuelve al prompt del sistema operativo.
<b>close</b>	Cierra la conexión del usuario activo, sin salirnos de la consola FTP.

#### Comandos para la gestión de los directorios

Comando	Descripción
<b>pwd</b>	Muestra la ruta de donde nos encontramos del equipo destino
<b>!pwd</b>	Muestra la ruta de donde nos encontramos del equipo local.
<b>cd</b>	Cambia de directorio en el equipo remoto
<b>lcd</b>	Cambia de directorio en el equipo local
<b>ls</b>	Lista la información del directorio del equipo destino.
<b>!ls</b>	Lista la información del directorio del equipo local.
<b>mkdir</b>	Crea un directorio en el equipo destino, si tiene permisos.
<b>!mkdir</b>	Crea un directorio en el equipo local.
<b>rmdir</b>	Elimina un directorio en el equipo destino si tiene permisos.
<b>!rmdir</b>	Elimina un directorio en el equipo local.

## Comandos para la gestión de ficheros

Comando	Descripción
<b>get [archivo]</b>	Recupera un archivo del equipo remoto y lo almacena en el equipo local
<b>mget [archivo]</b>	Recupera una lista de archivos, que cumplan un patrón, desde el equipo remoto al local.
<b>put [archivo]</b>	Transfiere un archivo del equipo local al remoto.
<b>mput [archivo]</b>	Transfiere una lista de archivos, que cumplan un patrón, del equipo local al remoto.
<b>binary</b>	Cambia el tipo de transferencia a binario.
<b>ascii</b>	Cambia el tipo de transferencia a texto.
<b>delete [archivo]</b>	Borra un archivo en el equipo destino si tiene permisos.
<b>mdelete</b>	Borra archivos, en base a un patrón, en el equipo remoto (si tiene permisos).

## 6 Configuración y uso de cuotas

Anteriormente se comentó el concepto de cuota y su importancia para el rendimiento del sistema.

En Linux, el administrador puede **establecer límites de forma individual a cada usuario o puede hacerlo para todo un grupo**.

Además, existen dos enfoques diferentes en el momento de establecer cuotas:

- **Limitar el número de bloques de disco**, con lo que se restringe el tamaño máximo que se puede ocupar.
- **Limitar el número de i-nodos**, que restringe el número máximo de archivos que pueden crearse. Un i-nodo guarda las características de un objeto del sistema de archivos (un archivo, un directorio, etc.). Por lo tanto, limitando su número limitamos la cantidad máxima de objetos.

Además, cuando un administrador establece cuotas, puede fijar dos tipos de límites:

- **Rígido (hard)**: El sistema operativo impedirá que el límite sea sobrepasado.
- **Flexible (soft)**: El sistema operativo avisará cuando el límite sea sobrepasado.

### 6.1 Instalar y configurar las cuotas de disco

Los pasos que deberemos seguir para hacer uso de las cuotas de disco en Ubuntu son los siguientes:

- Instalar los paquetes necesarios.
- Activar las cuotas en el sistema de archivos y volver a montarlo.
- Crear los archivos de cuota y la tabla de uso de espacio compartido.
- Configurar cuotas para usuarios y grupos.
- Establecer un valor para el periodo de gracia.

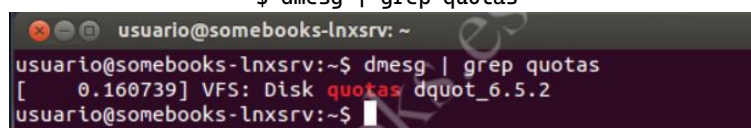
Una vez que tenemos claro el objetivo, comencemos...

#### 6.1.1 Instalar los paquetes necesarios.

Aunque la mayoría de las distribuciones GNU/Linux incorporan en su núcleo (kernel) la capacidad para manejar cuotas, puede que alguna de ellas no lo haga. Si nos encontráramos en ese caso, sería preciso volver a compilar el núcleo del sistema (cosa que, de momento, no forma parte de nuestros objetivos).

En cualquier caso, si estás utilizando una distribución diferente de Ubuntu, puedes comprobar que soporta cuotas ejecutando el siguiente comando:

```
$ dmesg | grep quotas
```



```
usuario@somebooks-lnxsrv: ~
usuario@somebooks-lnxsrv:~$ dmesg | grep quotas
[ 0.160739] VFS: Disk quotas dquot_6.5.2
usuario@somebooks-lnxsrv:~$
```

El comando dmesg (diagnostic message) muestra los mensajes generados por el proceso de arranque. Lo que hacemos con este comando es enviar la salida a grep para localizar la línea que hace referencia a las cuotas durante el arranque.

Lógicamente, si al ejecutar el comando no aparece ningún texto, significa que el núcleo no está preparado para manejar cuotas.

**Nota:** Si utilizas Ubuntu, el soporte para cuotas está incluido en el núcleo.

Una vez realizada esta comprobación, procederemos a instalar los paquetes necesarios para manejar las cuotas:

```
$ sudo apt-get install quota quotatool
```

```

usuario@somebooks-lnxsrv: ~
libnet-ldap-perl
Se instalarán los siguientes paquetes NUEVOS:
quota quotatool
0 actualizados, 2 se instalarán, 0 para eliminar y 245 no actualizados.
Necesito descargar 575 kB de archivos.
Se utilizarán 1.528 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu/ precise-updates/main quota i386 4.00-
3ubuntu1 [557 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu/ precise/universe quotatool i386 1.4.11-
1-1 [17,8 kB]
Descargados 575 kB en 0seg. (784 kB/s)
Preconfigurando paquetes ...
Seleccionando paquete quota previamente no seleccionado
(Leyendo la base de datos ... 147327 ficheros o directorios instalados actualmen-
te.)
Desempaquetando quota (de .../quota_4.00-3ubuntu1_i386.deb) ...
Seleccionando paquete quotatool previamente no seleccionado
Desempaquetando quotatool (de .../quotatool_1.4.11-1_i386.deb) ...
Procesando disparadores para man-db ...
Procesando disparadores para ureadahead ...
ureadahead will be reprofiled on next reboot
Configurando quota (4.00-3ubuntu1) ...
Configurando quotatool (1.4.11-1) ...
usuario@somebooks-lnxsrv:~$

```

Si todo es correcto, estamos listos para comenzar.

### 6.1.2 Activar las cuotas en el sistema de archivos y volver a montarlo

Para que el sistema pueda gestionar los valores de cuota de un dispositivo de almacenamiento, éste debe montarse teniendo en cuenta dicha característica. Los comandos **mount** y **umount** obtienen la información necesaria para montar cualquier dispositivo o partición del **archivo fstab** (file systems table). Por lo tanto, necesitaremos editar este fichero para incorporar la nueva característica.

Como es habitual, usamos el editor nano para editar el archivo **/etc/fstab** con privilegios de superusuario. En nuestro caso, asignaremos cuotas al directorio **/home** del sistema, por lo que buscaremos la línea que hace referencia al mismo.

```

usuario@somebooks-lnxsrv: ~
GNU nano 2.2.6 Archivo: /etc/fstab

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
proc /proc proc nodev,noexec,nosuid 0 0
# / was on /dev/sda5 during installation
UUID=0ebc7eee-5545-47ed-8ab1-6919482cfbb2 / ext4 errors=remount$
# /home was on /dev/sda6 during installation
UUID=24e18f86-beac-4f34-96a2-b6de5d33da71 /home ext4 defaults $
# swap was on /dev/sda1 during installation
UUID=2111f83a-c29e-4781-9d33-b3c8e6138539 none swap sw $

[ 14 líneas leídas ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^D Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografía

```

Una vez localizada, incluiremos los argumentos que informan al sistema de que el volumen indicado podrá tener cuotas para los usuarios y para los grupos (**usrquota** y **grpquota**), es decir, la línea quedará similar a:

```
UUID=24e18f86-beac-4f34-96a2-b6de5d33da71 /home ext4 defaults,usrquota,grpquota 0 2
```

Para que el sistema de cuotas esté activo, sólo nos quedará montar de nuevo la partición sobre la que se aplicarán las cuotas. Esto podemos conseguirlo fácilmente con el siguiente comando:

```
sudo mount -o remount,rw /home
```

Podemos usar el comando **mount** para comprobar que se ha cargado la nueva configuración

### 6.1.3 Crear los archivos de cuota y la tabla de uso de espacio compartido

El siguiente paso consistirá en preparar al sistema de archivos para que admita las cuotas. Para lograrlo, utilizaremos el comando **quotacheck**, que se encargará de examinar el sistema de archivo que le indiquemos y crear una tabla del uso actual del disco. Después, la compara con la información almacenada en los archivos de cuota de disco del sistema de archivos, actualizándolos cuando sea necesario.

En nuestro caso, como es la primera vez que usamos las cuotas, los archivos de cuota no existen en el sistema de archivos. Por este motivo, usaremos el **argumento -c**, que permite crearlos de forma automática (en realidad, han podido crearse automáticamente si reiniciaste al final del punto anterior).

```
sudo quotacheck -cgu /home
```

**Nota:** Los argumentos -g y -u hacen que se comprueben tanto los grupos como los usuarios

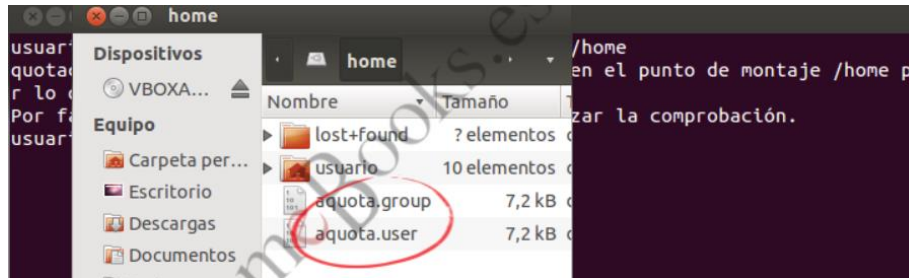
```

usuario@somebooks-lnxsrv: ~
usuario@somebooks-lnxsrv:~$ sudo quotacheck -cgu /home
quotacheck: Las cuotas para user están activadas en el punto de montaje /home po
r lo que quotacheck podría dañar el archivo.
Por favor, desactive las cuotas o use -f para forzar la comprobación.
usuario@somebooks-lnxsrv:~$

```

Si obtenemos un error como el que se observa en la imagen sólo significa que las cuotas ya se han activado.

También podemos comprobar que los archivos de cuotas (aquota.user y aquota.group) se han creado correctamente en el directorio en el que se ha establecido la cuota.



#### 6.1.4 Configurar cuotas para usuarios y grupos

Para asignar cuotas a los usuarios o grupos usaremos el **comando edquota**. Por ejemplo, para asignar valores de cuota a la cuenta usuario, escribiríamos lo siguiente:

```
sudo edquota -u usuario
```

Para asignar valores a todo un grupo, bastaría con escribir así el comando anterior:

```
sudo edquota -g grupo
```

En realidad, el **comando edquota** abre el editor nano con la información correspondiente a la cuota del usuario o grupo que hayamos indicado.

```

GNU nano 2.2.6      Archivo: /tmp//EdP.aq0qod9
Quotas de disco para user usuario (uid 1000):
Sist. arch.    bloques    blando    duro    inodos    bland$
/dev/sda6      3116        0         0       306       0$

```

El editor nos muestra la siguiente información, ordenada en columnas:

- **Sist. arch:** La partición para la que tenemos activadas las cuotas. En nuestro ejemplo es /dev/sda6, pero en otro equipo puede ser distinta.
- **Bloques:** Indica el número de bloques que está usando el usuario en estos momentos.
- **Blando / Soft:** Indica un valor flexible en cuanto al número de bloques utilizados. Este límite podrá sobrepasarse durante un determinado tiempo (**periodo de gracia**).
- **Duro / hard:** Representa el límite rígido de bloques que podrá usar el usuario (o grupo). Cuando el espacio ocupado por el usuario alcance el valor indicado en esta columna, ya no podrá guardar más información.
- **inodos:** Indica el número de i-nodos que está usando el usuario en estos momentos.
- **Blando / Soft:** Indica un valor flexible en cuanto al número de archivos y/o directorios utilizados. Como en el caso de los bloques, el límite podrá sobrepasarse durante un tiempo (**periodo de gracia**).
- **Duro /hard:** Representa el límite rígido de i-nodos que podrá usar el usuario (o grupo). Cuando el usuario alcance el número de archivos y/o directorios indicado en esta columna, ya no podrá crear archivos y/o directorios nuevos.

Cuando acabemos de establecer los valores adecuados, saldremos del editor pulsando las teclas **ctrl + x** y asegurándonos de guardar los cambios.

#### Nota:

Para eliminar cualquier límite, basta con poner su valor a cero.

La asignación de cuotas a grupos funciona de forma idéntica a la de los usuarios



### 6.1.5 Establecer un valor para el periodo de gracia

Como hemos comentado antes, el periodo de gracia representa el tiempo durante el cual podrá sobrepasarse un límite flexible antes de que se convierta en rígido.

El tiempo de gracia puede expresarse en días, horas, minutos o segundos.

Para modificar el valor predeterminado del periodo de gracia sólo debemos ejecutar el siguiente comando:

```
sudo edquota -t
```

Para cambiar el valor del periodo actuaremos como estableciendo las cuotas:

```
usuario@somebooks-lnxsr: ~
GNU nano 2.2.6 Archivo: /tmp//EdP.aXjBL7P

Periodo de gracia antes de imponer límites blandos para users:
La unidad de tiempo puede ser: días, horas, minutos, o segundos
Sist. arch.      Periodo gracia bloque  Periodo gracia inodo
/dev/sda6        7días                7días
```

Cuando acabemos de establecer los valores adecuados, saldremos del editor pulsando las teclas **ctrl + x** y asegurándonos de guardar los cambios.

**Nota:** Como puede verse, incluso podemos asignar valores diferentes para los bloques y para los i-nodos.

#### IMPORTANTE:

El comando `edquota` es capaz de cambiar las unidades de tiempo en inglés, por su traducción al español, para mostrarnos el archivo. Sin embargo, luego no es capaz de hacer la conversión contraria. Esto significa que, cuando escribamos los valores para los periodos de gracia, deberemos utilizar las unidades de tiempo en inglés (days, hours, minutes o seconds)

## 6.2 Comprobar las cuotas de disco

Si, en el futuro, necesitamos comprobar qué cuota le establecimos a un determinado usuario, sería tan fácil como usar el comando `edquota` y volver a editar el fichero de definición. Sin embargo, disponemos de otras opciones que nos evitan el riesgo de modificarlo por accidente:

El **comando quota** ofrece la información relativa a las cuotas de un usuario o grupo determinado. La sintaxis sería como en el siguiente ejemplo:

```
sudo quota -u <usuario>
sudo quota -u usuario
```

```
usuario@somebooks-lnxsr: ~
usuario@somebooks-lnxsr:~$ sudo quota -u usuario
Cuotas de disco para user usuario (uid 1000):
Sistema de archivos bloques  quota límite  graciaarchivos  quota límite  gracia
a
/dev/sda6 3132 3200 3250 309 0 0
usuario@somebooks-lnxsr:~$
```

Como puedes suponer, para consultar la cuota de un grupo, la sintaxis sería así:

```
sudo quota -g <grupo>
sudo quota -g daw2
```

**Nota:** Si omitimos los argumentos `-u` o `-g`, el comando supondrá que estamos consultando la cuota de un usuario.

El **comando repquota** muestra un informe sobre el grado de ocupación y las cuotas en una determinada partición. La sintaxis sería así:

```
sudo repquota <punto montaje>
sudo repquota /home
```

```
usuario@somebooks-lnxsr: ~
usuario@somebooks-lnxsr:~$ sudo repquota /home
*** Informe para user quotas en dispositivo /dev/sda6
Periodo de gracia de bloque: 7días; periodo de gracia de inodo: 7días
límites de Bloque      Límites de archivo
Usuario  usado  blando  duro gracia  usado  blando  duro gracia
-----
root    --    20     0     0           2     0     0
usuario --   3132  3200  3250       309     0     0
ltoro   --    28    50    60           5     0     0
```

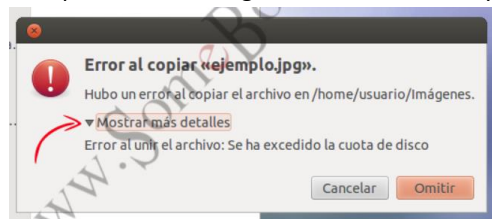
Un detalle que pasa casi desapercibido en el informe anterior son los dos guiones (--) que hay después del nombre de usuario. El primero indica que aún no se ha excedido el límite flexible para los bloques y el segundo que no se ha excedido el límite flexible en los i-nodos. Cuando se exceda cualquiera de ellos, su guión se convertirá en un signo más (+). Además, también aparecerá el periodo de gracia que aún tendrá el usuario para seguir excediendo el límite. Ver ejemplo en la siguiente imagen:

```

usuario@somebooks-lnxsrv:~$ sudo repquota /home
*** Informe para user quotas en dispositivo /dev/sda6
Periodo de gracia de bloque: 7días; periodo de gracia de inodo: 7días
límites de Bloque          Límites de archivo
-----
Usuario  usado  blando  duro gracia  usado blando duro gracia
-----
root     --    20      0      0             2      0      0
usuario  +-   3248   3200   3250 6días      462      0      0
ltoro    --    28      50      60             5      0      0
    
```

Como puedes intuir, este es un mecanismo muy sencillo para identificar a los usuarios que han excedido alguno de sus límites, cuando el número de usuarios es elevado.

Por último, cuando un usuario trate de sobrepasar su límite rígido, recibirá un error y la operación no podrá completarse.



### 6.3 Desactivar y volver a activar las cuotas.

En ocasiones, podemos necesitar desactivar las cuotas de forma transitoria, por ejemplo, para realizar alguna operación administrativa, y volver a activarlas más tarde.

Desactivarlas será tan sencillo como escribir el comando: **quotaoff**

```
sudo quotaoff /home
```

Para volverlas a activar, bastará con utilizar el comando **quotaon**:

```
sudo quotaon /home
```

## 7 Protocolo seguro de transferencia de archivos

La instalación que se va a realizar es el servidor FTP en modo seguro con certificado y configurado en el fichero `tls.conf` para SO Linux bajo la versión de Debian.

El procedimiento de instalación es el siguiente:

1. El primer paso es descomentar la línea que permite incluir el fichero `tls.conf` para configurar la conexión segura:
 

```
#include /etc/proftpd/tls.conf
```
2. Posteriormente, habría que eliminar el comentario en las siguientes líneas del fichero `tls.conf` para comprobar que funciona la seguridad en la conexión con el servidor FTP.

```

#IfModule mod_tls.c>
#    TLSEngine
#    TLSLog /var/log/proftpd/tls.log
#    TLSProtocol
#    TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
#    TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key
    
```



- El siguiente paso es **generar las claves públicas** que se colocarán en la ruta **/etc/ssl** mediante el comando **proftpd-gencert**

```

root@osboxes:/etc/proftpd# proftpd-gencert
Generating a 2048 bit RSA private key
.....+++++
writing new private key to '/etc/ssl/private/proftpd.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Cordoba
Locality Name (eg, city) []:Cordoba
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Educacion
Organizational Unit Name (eg, section) []:Practica
Common Name (e.g. server FQDN or YOUR name) []:FTP
Email Address []:

Use the following information in your ProFTPD configuration:

TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key
    
```

- A continuación, se va a proceder a dar los permisos adecuados a los ficheros generados:  
`#chmod 600 /etc/ssl/private/proftpd.key`  
`#chmod 644 /etc/ssl/certs/proftpd.crt`
- Por último, reiniciamos el servidor FTP con el comando siguiente. Y obtendremos la conexión segura con certificado, como se puede observar en la imagen adjunta:

`#service proftpd restart`

El certificado del servidor es desconocido. Por favor, examine cuidadosamente el certificado para asegurarse de que se puede confiar en el servidor.

Detalles	
Desde válido:	30/03/20 14:26:37
Válido hasta:	30/03/21 14:26:37
Número de serie:	00:db:a0:9c:0a:30:9a:75:14
Algoritmo de clave pública:	RSA con 2048 bits
Algoritmo de firma:	RSA-SHA256
Huella digital (SHA-256):	66:57:35:cc:b3:79:55:0e:79:07:11:ed:ab:02:c2:90: f6:56:3f:c7:0e:a8:e1:42:0b:4a:63:8a:32:21:b4:3a
Huella digital (SHA-1):	0d:f0:f2:fb:ad:11:db:a1:a7:87:13:ca:9a:fd:78:82:57:d0:51:fc

Asunto del certificado	Agente de certificado
Nombre común: FTP	Nombre común: FTP
Organización: Educacion	Organización: Educacion
Unidad: Practica	Unidad: Practica
País: ES	País: ES
Estado o provincia: Cordoba	Estado o provincia: Cordoba
Localidad: Cordoba	Localidad: Cordoba

Detalles de la sesión		
Sitio:	10.0.2.15:21	
Protocolo:	TLS1.3	Cifrado: AES-256-GCM
Intercambio de clave:	ECDHE-RSA	MAC: AEAD

## 8 VirtualHosts en ProFTP

Los **Virtual Hosts** nos permiten tener diferentes servidores FTP en un mismo equipo, reduciendo considerablemente los costes de hardware y su mantenimiento. Al igual que ocurre con el servidor Web de Apache, el cuál veremos en un tema posterior, con ProFTPD podemos configurar varios servidores FTP en un mismo equipo y con configuraciones totalmente diferentes.

El término Virtual Host se refiere a hacer funcionar más de un sitio (ftp,web etc ...) como por ejemplo `www.servidor1.com` y `www.servidor2.com` en una misma máquina. Los Hosts Virtuales pueden funcionar basándose en "direcciones IP", lo que significa que cada Virtual Host tiene una dirección IP diferente, o basados en "nombres de dominio", lo que significa que con una sola dirección IP están funcionando Virtual Hosts con diferentes nombres de dominio. Este proceso es totalmente transparente para el usuario final.

Vamos a ver un ejemplo en el que configuraremos un host virtual para que atienda las peticiones FTP de los clientes. En este caso el nombre del servidor será ftp.servidor1.com.

Para establecer la nueva configuración, realizaremos las siguientes acciones:

1. Accedemos al fichero /etc/proftpd/proftpd.conf  
# nano /etc/proftpd/proftpd.conf
2. Activamos / descomentamos la línea:  
#include /etc/proftpd/virtuals.conf  
Con ello permitimos que se incluya el fichero que nos va a permitir trabajar con host virtuales.
3. Añadimos la directiva <VirtualHost> con la configuración que deseamos para dicho servidor

En nuestro caso podríamos tener algo como

```
<VirtualHost ftp.servidor1.com>
    ServerAdmin          admin@servidor1.com
    ServerName            "FTP - Servidor1"
    AuthUserFile          /etc/proftpd/passwd.virtuales
    MaxLoginAttempts      3
    RequireValidShell     no
    DefaultRoot           /var/ftp/bbdd
    AllowOverwrite        yes
</VirtualHost>
```

Donde:

- **ServerAdmin:** sirve para añadir el e-mail del administrador.
  - **ServerName:** Nombre del servidor FTP.
  - **AuthUserFile:** fichero de autorización de usuarios virtuales.
  - **MaxLoginAttempts:** número máximo de intentos fallidos.
  - **RequireValidShell:** se usa para confirmar si se quiere que el usuario pertenezca al sistema operativo.
  - **DefaultRoot:** ruta en la que se ubicará el usuario de FTP cuando se conecte.
  - **AllowOverwrite:** para poder escribir en la ruta anterior.
4. Para aplicar los cambios, reiniciamos el servicio.  
#service proftpd restart