

# Very Secure FTP Daemon (vsftpd)

## Configuración básica

### Configuración del servicio de transferencia de archivos

---

Desde Linux lo primero es actualizar los repositorios para luego instalar el servidor.

```
sudo apt-get update
sudo apt-get install vsftpd
```

Podemos ver que se ha añadido un script de autoarranque

```
sudo nano /etc/init.d/vsftpd
```

Podemos probar que todo haya ido bien mediante el cliente en modo texto

```
ftp localhost
```

lo que nos pedirá unas credenciales para acceder. Por defecto nos conectamos como el usuario *anonymous* y sin contraseña.

El archivo de configuración de **vsFTPD** se puede consultar como viene siendo habitual.

```
sudo nano /etc/vsftpd.conf
```

El parámetro `ftpd_banner` sirve para establecer el banderín de bienvenida que será mostrado cada vez que un usuario acceda al servidor. Puede establecerse cualquier frase breve que consideres conveniente:

```
ftpd_banner=Bienvenido al servidor FTP de DAW
```

Tras cada cambio en la configuración es necesario reiniciar el servidor.

```
sudo service vsftpd restart
```

### Usuarios anónimos

---

Por defecto nuestra instalación sólo permite conexión con un usuario local de Linux:

```
anonymous_enable=NO
local_enable=YES
```

Para activar los usuarios anónimos lo único que tenemos que hacer es cambiar la directiva y reiniciar el servidor:

```
anonymous_enable=YES
```

El directorio por defecto para el usuario anónimo es `/srv/ftp/` y para los usuarios regulares su carpeta personal `/home/%user%/`.

Creamos la carpeta y nos aseguramos de que tenga el propietario y los permisos adecuados.

```
mkdir /srv/ftp/pub/upload  
chown root.root /srv/ftp/pub/upload/  
chmod 757 /srv/ftp/pub/upload/
```

Cuando intentamos conectarnos puede darnos un error 500. Esto se debe a que el usuario no debe tener permisos de escritura en su carpeta raíz así que podemos quitárselos y ya está. Por ello ahora tendrá que escribir dentro de *upload*.

```
chmod 555 /srv/ftp/pub
```

También hay que modificar una directiva para que se permitan subir archivos al servidor y recargar la configuración:

```
write_enable=YES  
allow_writeable_chroot=YES
```

y un poco más abajo configuramos que los usuarios anónimos puedan subir archivos y que puedan crear directorios:

```
anon_upload_enable=YES  
anon_mkdir_write_enable=YES
```

reiniciamos el servidor ftp y probamos.

Si queremos volver a desactivar la opción de que los usuarios anónimos puedan usar subir archivos, simplemente tenemos que comentar las dos últimas directivas, pero mantenemos la opción de que los usuarios corrientes puedan subir archivos.

Un grave problema de seguridad en FTP y Linux (no solo con vsFTPd) es que un usuario tiene acceso a toda la estructura de archivos del servidor. Aunque no tenga permisos para escribir puede leer y listar... La forma fácil de solucionarlo es

```
chroot_local_user=YES
```

No es **nada recomendable** modificar el directorio por defecto `/srv/ftp/` ya que puede suponer un gran agujero de seguridad por el que se cuelen muchísimos ataques a nuestro servidor. Aun así, si queremos cambiar la carpeta raíz de los usuarios anónimos, escribiremos la directiva correcta en `vsftpd.conf` y crearemos el directorio:

```
mkdir /var/ftpcomp/pub  
anon_root=/var/ftpcomp/pub
```

## Usuarios locales

---

Creamos un usuario en Linux:

```
sudo adduser usuario
```

Vamos a la carpeta `/home/` y le daremos permisos para que sea el dueño de su depósito en el ftp:

```
sudo chown usuario.ftp usuario
```

Habilitamos el **enjaulamiento** de los usuarios dentro de su directorio personal y también para acceder a sus carpetas por FTP quitando `#`.

```
chroot_local_user=YES
```

También podemos activar y editar la lista en donde los usuarios van a estar enjaulado:

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

## Permisos y cuotas

---

Para tener un control de cuotas, podemos agregar algunas opciones al final del archivo de configuración del servidor:

```
anon_max_rate=5100      #Ancho de banda para usuario anónimo 5kb.  
local_max_rate=5100     #Ancho de banda por usuario local 5kb.  
max_clients=3           #Número máximo clientes conectados.  
max_per_ip=2            #Número máximo de conexiones por ip.
```