

HOWTO

Manual para configurar un Servidor FTP con Vsftpd en openSUSE



Índice de contenido

INTRODUCCIÓN.....	3
INSTALACIÓN.....	3
CONFIGURACIÓN BÁSICA.....	4
Configuraciones Generales:.....	4
Configuración para usuarios Locales:.....	5
Configuración para usuarios Anónimos:.....	5
Configuración de logs:.....	6
Configuraciones relacionadas a Transferencias:.....	6
USUARIOS VIRTUALES.....	8
CONEXIONES SEGURAS UTILIZANDO SSL.....	11
ENLACES.....	12
ANEXOS.....	12
1.Cambiar directorio raíz de Usuarios Virtuales del servicio FTP.....	12

INTRODUCCIÓN

Este pequeño documento tiene como objetivo indicar los principales pasos para configurar un servicio ftp en openSUSE utilizando el reconocido servidor VSFTPD(Very Secure FTPD).

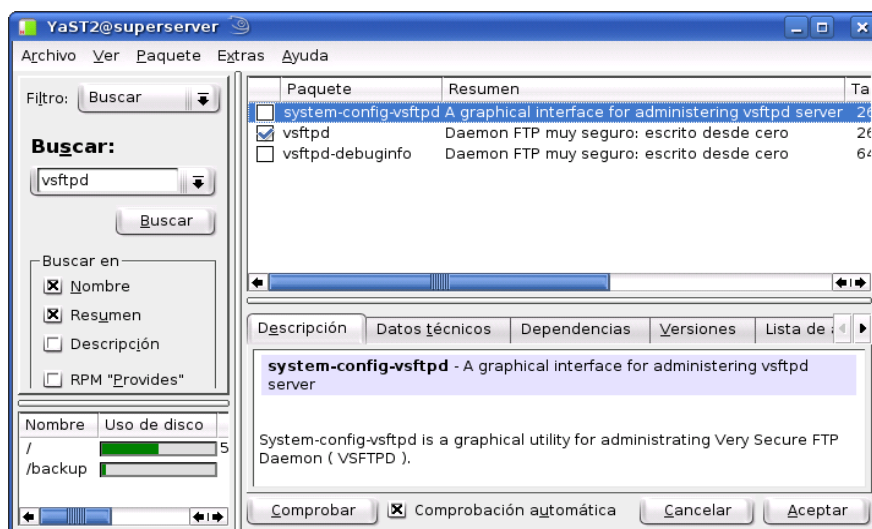
Aclaro que en la mayoría de los casos las configuraciones son realizadas editando directamente los archivos de configuración, para esto pueden utilizar el editor de texto de su preferencia (Yo utilizo el Vim =)).

Acerca de las Pruebas: Los pasos de configuración fueron probados en dos equipos:

- Equipos de Prueba:
 1. Intel Pentium III 550 Mhz. / Mem. 384Mb / HD 40Gb. / Placa Asus
 2. Notebook Acer / AMD Turion 64 x2 1.6Ghz. / Mem. 2 Gb. / HD 120 Gb.
- Distribuciones Utilizadas: openSUSE 10.3 i586 y openSUSE 10.3 x86_64 respectivamente.
- Versión utilizada del Servidor Vsftpd: 2.0.5-78

INSTALACIÓN

Para instalar el paquete del servidor VSFTPD lo hacemos desde “Yast → Software → Instalar/desinstalar Software” donde buscamos el paquete con nombre “vsftpd”, lo seleccionamos, comprobamos las dependencias y lo instalamos.



Todas los demás paquetes que necesitaremos más adelante posiblemente ya han sido instalados por defecto con el sistema operativo (paquetes pam, openssl, openssl-certs, db-utils, etc.) ya que son paquetes fundamentales para otras aplicaciones básicas, no obstante, podemos verificar su instalación desde Yast.

Cuando hayamos culminado con la instalación probamos levantar el servicio abriendo una consola en la cual nos conectamos como super usuario (`gabriel@superserver:~> su -`) y ejecutamos el siguiente comando:

```
superserver:/ # service vsftpd start
```

si el servicio se levantó correctamente saldrá el siguiente mensaje:

```
Starting vsftpd           done
```

Paramos nuevamente el servicio con el comando `service vsftpd stop`, accedemos nuevamente al Yast y nos dirigimos a “Sistema → Editores de niveles de ejecución” donde verificamos que en modo experto estén marcadas las opciones 3 y 5 de los niveles de ejecución para el servicio vsftpd, lo que permite que el servicio se inicie automáticamente cada vez que se encienda el equipo. Concluido con estos pasos, continuamos con la configuración del servicio en sí.

CONFIGURACIÓN BÁSICA

El archivo de configuración del servidor VSFTPD se encuentra en el directorio `/etc/` y se llama `vsftpd.conf`, el cual vamos a tener que modificar con cualquier editor de texto que sea de nuestra preferencia.

Las directivas o comandos que se van a especificar en esta sección son las necesarias para montar un servidor ftp básico que permite la conexión de usuarios locales del sistema operativo como así también de usuarios anónimos.

Obs: Antes de comenzar a modificar un archivo de configuración, nunca hay que olvidarse de hacer una copia de seguridad del mismo, así siempre tendremos a mano una versión original para restaurar la configuración por defecto sin perder mucho tiempo ;).

Abrimos el archivo conectados como root:

```
superserver:/ # vi /etc/vsftpd.conf
```

A continuación se citarán las principales directivas que deberán estar definidas (descomentadas) en el archivo de configuración seguidos de sus respectivos parámetros, hay muchas otras directivas que se pueden consultar en http://vsftpd.beasts.org/vsftpd_conf.html, toda línea que lleve al principio el carácter almohadilla (#) será interpretado como un simple comentario.

Configuraciones Generales:

```
#!/bin/bash
# Ejemplo del archivo de configuración /etc/vsftpd.conf
# General Settings
#
# Permite el modo escritura.
write_enable=YES

# Activa mensajes de directorio.
dirmessage_enable=YES
```

```
# Mensaje de bienvenida
ftpd_banner=Bienvenido al servidor ftp de GK - Powered by openSuSE 10.3
```

Configuración para usuarios Locales:

```
# Local FTP user Settings
#
# Permite que usuarios locales puedan conectarse.
local_enable=YES

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

# Permite especificar una lista con los usuarios locales a los cuales no
# se les enjaulará cuando la opción chroot_local_user = YES.
chroot_list_enable=YES

# Especifica la ruta en donde se encuentra la lista, en mi caso he creado una
# carpeta en el directorio /etc llamada "vsftpd", en la cual coloqué el archivo
# de texto (vsftpd.chroot_list) que contiene la lista.
chroot_list_file=/etc/vsftpd/vsftpd.chroot_list

# Esta directiva la he dejado comentada, pero puede resultar muy interesante
# para los casos en que sea necesario limitar la velocidad de transferencia para
# los usuarios locales, por defecto la velocidad de transferencia es ilimitada.
#local_max_rate=7200
```

Configuración para usuarios Anónimos:

La configuración que viene más adelante está ideada para que los usuarios que se conectan anónimamente, no puedan subir archivos, sino solamente descargar aquellos compartidos por el administrador del servicio.

Antes de comenzar con la modificación de las directivas de la sección "Anonymus FTP user settings" del archivo vsftpd.conf, necesitamos crear una carpeta en el sistema de archivos que será utilizada como el directorio raíz para las conexiones anónimas, con la instalación por defecto del servidor vsftpd en openSUSE 10.3, el directorio para usuarios anónimos se encuentra por defecto en /srv/ftp/, este directorio es el HOME del usuario de sistema "ftp" dueño del servicio (Ver Yast → Seguridad y Usuarios → Gestión de Usuarios → Definir Filtro: Usuarios del Sistema → Usuario FTP → Ver Detalles). Previendo la posterior utilización de dicho directorio para albergar a los usuarios virtuales, coloqué una nueva carpeta en dicho directorio llamada anónimo (/srv/ftp/anonimo) :

```
superserver: # cd /srv/ftp
```

```
superserver:/srv/ftp # mkdir anonimo
```

asignándole el dueño:grupo y los permisos de forma idéntica a la carpeta "ftp" que se encuentra en /srv, esto lo comento porque cuando coloqué otros permisos a la carpeta "anonimo", las conexiones anónimas no funcionaron correctamente.

```
superserver:/srv/ftp # chmod 755 anonimo/
```

```
superserver:/srv/ftp # chown root:root anonimo/
```

Esta carpeta (/srv/ftp/anónimo) será la que contendrá los archivos compartidos para los usuarios conectados como anónimos.

Continuación de la configuración del archivo vsftpd en la sección “Anonymus FTP user Settings”:

```
# Anonymus FTP user Settings
#
# Permitir conexiones anónimas.
anonymous_enable=YES

# Directorio raíz para los usuarios anónimos. Carpeta creada en /srv/ftp/ como
# se comentó anteriormente.
anon_root=anonimo

# Solo permite descargar a los usuarios anónimos aquellos archivos que tengan
# permisos de lectura.
anon_world_readable_only=YES

# Para mi caso especifiqué con la siguiente directiva que los usuarios anónimos
# no tengan permisos para subir archivos al servidor.
anon_upload_enable=NO

# Esta directiva permite a los usuarios anónimos a crear carpetas en ciertos
# casos.
anon_mkdir_write_enable=NO

# Directiva que permite establecer el límite de la velocidad máxima de
# transferencia de datos para los usuarios anónimos. Fui un poco drástico jeje
# (2kb/s)
anon_max_rate=2048
```

Configuración de logs:

```
# Log Settings
#
# Activa la generación de registros logs por cada uploads/downloads.
xferlog_enable=YES

# Define cual será el archivo log.
vsftpd_log_file=/var/log/vsftpd.log

# Si esta directiva no se encuentra comentada activa el registro (log) de todas
# las peticiones/respuestas del servidor.
log_ftp_protocol=YES
```

Configuraciones relacionadas a Transferencias:

```
# Transfer Settings
#
# (ftp-data).
connect_from_port_20=YES

# Tiempo de espera para mantener establecidas conexiones inactivas.
idle_session_timeout=600
```

```
# Tiempo de espera para mantener establecidas conexiones de datos inactivas.
data_connection_timeout=120

# Comando que permite activar/desactivar conexiones pasivas.
pasv_enable=YES

# PAM setting. Suele estar configurado por defecto.
pam_service_name=vsftpd

# Configura listen=YES para que vsftpd corra en modo standalone.
listen=YES

# Máximos clientes simultáneos conectados. Ejemplo:
max_clients=5

# Máximas conexiones simultáneas por IP. Ejemplo:
max_per_ip=3

# Como tenemos activado el uso de conexiones pasivas especificamos el rango de
# puertos que serán utilizados por este método de conexión.
pasv_min_port=40000
pasv_max_port=40020
```

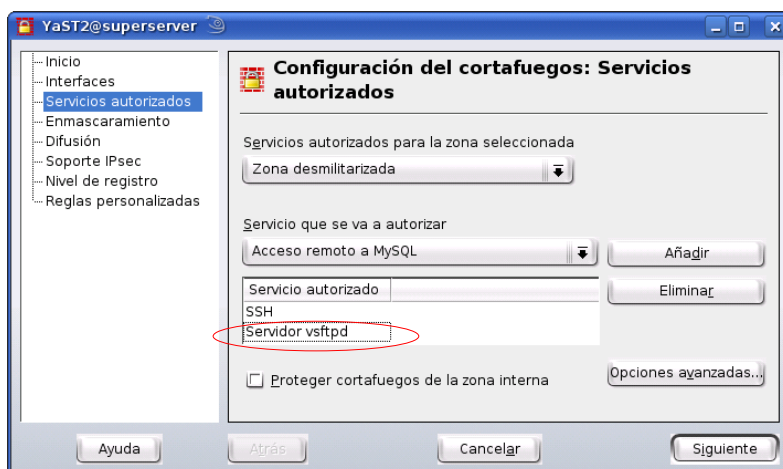
Bueno, hasta este punto ya tenemos configurado un servidor ftp básico que acepta conexiones de usuarios locales que pueden realizar downloads & uploads así como también acepta conexiones de usuarios anónimos que solamente tienen autorización para realizar descargas. Para poner nuevamente en marcha el servicio guardamos y salimos del archivo de configuración y ejecutamos el comando:

```
superserver:/ # service vsftpd start
```

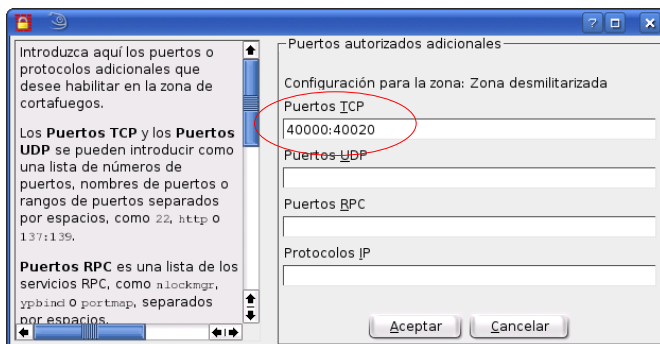
y si todo salió según lo planeado deberá aparecer una línea que indique que el servicio se inició correctamente:

```
Starting vsftpd           done
```

No hay que olvidarse de autorizar los puertos correspondientes al servicio vsftpd y del rango de puertos destinados a las conexiones pasivas en el Firewall de openSUSE en el caso de que el mismo se encuentre activo.



Servicio vsftpd autorizado en el firewall.



Rangos de puertos para conexiones pasivas autorizados en la ventana de Opciones Avanzadas.

USUARIOS VIRTUALES

Vamos a incorporar un punto más a favor de la seguridad evitando usar los usuarios locales para conectarnos al servidor ftp, para ello vamos a implementar el método de autenticación combinando PAM y bases de datos db (Berkeley Database) que son muy simples de manipular, para ello necesitamos tener instalados los paquetes db-utils y pam, que ya suelen estar instalados por defecto.

Para generar la tabla que contendrá los usuarios virtuales y sus respectivas contraseñas primeramente debemos crear un archivo de texto plano donde cargaremos esos datos, para ello nos dirigimos al directorio `/etc/vsftpd` que creamos anteriormente, ahí adentro creamos un nuevo archivo llamado por ejemplo `logins.txt`

```
superserver:/etc/vsftpd # touch logins.txt
```

le establecemos permisos de lectura y escritura solo para el usuario root con el comando:

```
superserver:/etc/vsftpd # chmod 600 logins.txt
```

y le agregamos un contenido similar a:

```
user_gabriel
pass_gabriel
user_jorge
pass_jorge
```

donde la primera línea corresponde al login del usuario virtual gabriel y la segunda a la contraseña del mismo, ya en la tercera línea se agrega otro nuevo login, en este caso jorge y que sigue el mismo procedimiento que las 2 primeras líneas (Arriba login y abajo la contraseña). Una vez que hayamos ingresado todos los usuarios virtuales que deseamos, preparamos un script que ejecutará una serie de comandos para generar la tabla db que es interpretable por el módulo pam.

Para el script creamos otro nuevo archivo también en el directorio `/etc/vsftpd/` llamado “generar_db.sh” y le agregamos el siguiente texto:

```
#!/bin/bash
# PRIMERAMENTE SE BORRA EL ARCHIVO "vsftpd_login.db" si es que ya existe.
rm -f vsftpd_login.db

# Genera el archivo "db" que contiene los usuarios virtuales
# del servicio vsftpd.
db_load -T -t hash -f logins.txt vsftpd_login.db

# Se asignan permisos de seguridad solo para root.
chmod 600 vsftpd_login.db
```

le asignamos el permiso de ejecución al archivo “generar_db.sh”:

```
superserver:/etc/vsftpd # chmod 700 generar_db.sh
```

y luego ejecutamos el script:

```
superserver:/etc/vsftpd # ./generar_db.sh
```

Con esto creamos el archivo “vsftpd_login.db” en el directorio `/etc/vsftpd/`, listo para ser utilizado.

El siguiente paso consiste en modificar el archivo de configuración PAM del servicio vsftpd, este archivo lo podemos encontrar en el directorio `/etc/pam.d/` y debería llevar el mismo nombre especificado en la directiva “`pam_service_name`”, en este caso “`vsftpd`”.

Antes de editar el archivo, hacemos una copia de seguridad del mismo y nos aseguramos que el servicio ftp no esté corriendo, verificado esto, editamos el archivo comentando todas sus líneas anteponiendo el carácter #, y le agregamos las siguientes líneas:

```
# Para usuarios virtuales. OBS: En caso de que se utilice un OS con arquitectura
# 64 bits (x86_64), la ruta correcta para el archivo "pam_userdb.so" es
# "/lib64/security/pam_userdb.so".
auth required /lib/security/pam_userdb.so db=/etc/vsftpd/vsftpd_login
account required /lib/security/pam_userdb.so db=/etc/vsftpd/vsftpd_login
```

Estas líneas permiten que los usuarios que se conecten al servicio ftp sean validados contra los registros que contiene la tabla `vsftpd_login.db` que hemos creado.

Como de ahora en más ya no se podrá acceder con los usuarios locales, se tiene que especificar al servidor vsftpd que un usuario local se encargará de gestionar todos los usuarios virtuales que se conecten, también aprovecharemos para agregar el directorio de donde el servidor vsftpd tendrá que buscar la configuración personal de cada usuario virtual, para lo que nuevamente editamos el archivo de configuración `/etc/vsftpd.conf` y agregamos las siguientes líneas al final del archivo:

```
# Usuarios Virtuales
#
# Activamos el uso de usuarios virtuales.
guest_enable=YES
```

```
# Esta directiva permite especificar el usuario que se encargará de manejar los
# usuarios Virtuales, por defecto si no se especifica esta línea en openSUSE es
# "ftp" que como ya sabemos tiene su home en /srv/ftp/, pero puede ser cualquier
# otro usuario si lo deseamos.
guest_username=ftp

# Especificamos el directorio de donde el servicio obtendrá la configuración
# personal de cada usuario virtual que agregamos a la tabla "vsftpd_login.db".
user_config_dir=/etc/vsftpd/config_por_usuario
```

Guardamos los cambios del archivo vsftpd.conf y creamos el directorio indicado en la directiva "user_config_dir" dentro de la carpeta /etc/vsftpd/:

```
superserver:/etc/vsftpd # mkdir config_por_usuario
```

En su interior creamos por cada usuario virtual que agregamos a la tabla "vsftpd_login.db" un archivo de texto plano con el mismo nombre del login del usuario.

```
superserver:/etc/vsftpd/config_por_usuario # touch gabriel jorge
```

Por ejemplo editamos el archivo "gabriel" recientemente creado y le agregamos las siguientes líneas:

```
#!/bin/bash
# Indicamos cual será el directorio personal del usuario gabriel
local_root=/srv/ftp/gabriel
# Le damos permisos de escritura para su directorio personal.
write_enable=YES
# Con virtual_use_local_privs igualado a YES, supone indicar que los usuarios
# virtuales tendrán los mismos privilegios que los usuarios locales.
virtual_use_local_privs=YES
```

Lo mismo podemos agregar al archivo "jorge", obviamente indicando otro directorio personal. Ahora solo nos resta crear los directorios personales para ambos usuarios virtuales (gabriel y jorge) en el directorio /srv/ftp/, cambiarlos de dueño y asignar los permisos correspondientes:

```
superserver: # cd /srv/ftp
superserver:/srv/ftp # mkdir gabriel jorge
superserver:/srv/ftp # chown -R ftp:ftp gabriel
superserver:/srv/ftp # chown -R ftp:ftp jorge
superserver:/srv/ftp # chmod -R 744 gabriel
superserver:/srv/ftp # chown -R 744 jorge
```

El siguiente paso es activar nuevamente el servicio (`service vsftpd start`) para comprobar su funcionamiento con los usuarios virtuales que hemos agregado, además las conexiones anónimas deberán seguir funcionando, solamente los usuarios locales ya no podrán conectarse al servidor.

CONEXIONES SEGURAS UTILIZANDO SSL

Como el protocolo ftp no encripta la información que fluye entre la aplicación cliente y el servidor, los datos como ser contraseñas, logins, etc. pueden ser obtenidos con mucha facilidad por personas con malas intenciones o simplemente curiosos mediante el escaneado de paquetes que circulan a través de la red. Para evitar estos casos, se puede activar la encriptación de paquetes utilizando ssl para tener un servicio ftp seguro (ftps).

El primer paso consiste en generar un Certificado SSL, para ello necesitamos tener instalados los paquetes openssl y openssl-certs. Nos dirigimos al directorio /etc/ssl/certs y ahí ejecutamos el siguiente comando:

```
superserver:/etc/ssl/certs# openssl req -x509 -nodes -days 7300 -newkey rsa:2048  
-keyout /etc/ssl/certs/vsftpd.pem -out /etc/ssl/certs/vsftpd.pem
```

Para preparar el certificado, el comando openssl nos solicitará que ingresemos varios datos como ser país, provincia, ciudad, empresa, nombre, email, etc., esta información luego aparecerá en el certificado que cualquier usuario deberá aceptar para hacer uso del protocolo seguro. Cuando finalice tendremos el certificado concluido con el nombre vsftpd.pem.

Para el siguiente paso paramos el service ftp en el caso de que lo tengamos corriendo (service vsftpd stop) y editamos el archivo de configuración vsftpd.conf, nos dirigimos hasta el final donde agregaremos las siguientes líneas

```
# Secure FTP  
#  
# Activamos el soporte SSL  
ssl_enable=YES  
  
# No se obliga el establecimiento de conexiones encriptadas mediante SSL para  
# usuarios locales.  
force_local_logins_ssl=NO  
  
# No se obliga a que las transferencias de datos locales sean encriptados con  
# SSL.  
force_local_data_ssl=NO  
  
# Se habilitan los soportes para las diversas versiones de SSL  
ssl_tlsv1=YES  
ssl_sslv2=YES  
ssl_sslv3=YES  
  
# Se especifica la ubicación del Certificado Generado.  
rsa_cert_file=/etc/ssl/certs/vsftpd.pem
```

Por ultimo iniciamos nuevamente el servicio vsftpd (service vsftpd start) y probamos establecer conexiones seguras utilizando clientes que soportan esta funcionalidad como ser los clientes FilleZilla, gFTP, etc.

ENLACES

Sitio Web de Vsftpd: <http://vsftpd.beasts.org/>

Completa Lista de Directivas para el archivo vsftpd.conf: http://vsftpd.beasts.org/vsftpd_conf.html

ANEXOS

1. Cambiar directorio raíz de Usuarios Virtuales del servicio FTP

La siguiente configuración muestra como cambiar el `root_local`(directorio raíz) original (`/srv/ftp`) para todos los usuarios virtuales a otro lugar, específicamente a un directorio de un usuario local como por ejemplo `/home/gabriel/descargas`.

Tomando en cuenta la configuración de usuarios virtuales que comenté en el manual, tuve que modificar y agregar unas cositas al archivo `vsftpd.conf` que muestro a continuación:

Primeramente cambie la directiva `guest_username` para colocarle el usuario local que manejará los usuarios virtuales y en cuyo home estará la carpeta raíz para los mismos, después le comenté con “#” la línea de la directiva `user_config_dir` para que ya no busque las configuraciones específicas de cada usuario virtual y por último le agregué dos nuevas líneas, una para especificar el directorio raíz con la directiva `local_root` y la otra para que le otorgue a los usuarios virtuales los mismos privilegios que tienen los usuarios locales con la directiva `virtual_use_local_privs=YES`. El archivo `vsftpd.conf` en la sección de usuarios virtuales me quedó como sigue:

```
# Usuarios Virtuales
#
# Activamos el uso de usuarios virtuales.
guest_enable=YES
#
# Esta directiva permite especificar el usuario que
# se encargará de manejar los usuarios Virtuales.
guest_username=gabriel
#
# Especificamos el directorio de donde el servicio obtendrá
# la configuración personal de cada usuario virtual que
# agregamos a la tabla "vsftpd_login.db". ESTA LINEA
# LA COMENTE PARA QUE NO SEA INTERPRETADA.
#user_config_dir=/etc/vsftpd/config_por_usuario
#
# Directorio raíz para usuarios registrados en vsftpd_login.db
# a partir del home de tu usuario local, en mi caso la carpeta
# estará en "/home/gabriel/descargas"
local_root=descargas
#
# Esta directiva ya es conocida y supone indicar que los usuarios virtuales
tendrán los
# mismos privilegios que los usuarios locales.
virtual_use_local_privs=YES
```

Con eso el archivo *vsftpd.conf* ya tiene todo lo que necesita, solo resta verificar que exista el directorio descargas, en mi caso lo tuve que crear sin necesidad de asignarle ningún permiso (por defecto 755 está ok) ni cambiarle de dueño:

```
gabriel@superserver:~> mkdir descargas
```

Por último hay que reiniciar el servicio y la nueva configuración debería funcionar sin problemas.

También se puede redirigir el directorio raíz para las conexiones anónimo al mismo directorio en donde los usuarios locales o virtuales suben sus archivos modificando la directiva *anon_root*:

```
anon_root=/home/gabriel/descargas
```

Así los usuarios anónimos podrán descargar los archivos que subieron los demás.