

Instalación de Servidor FTP vsftpd en Debian

- [Introducción y manual de instalación de vsftpd.](#)
- [vsftpd configuration parameters list](#)
- [Otro manual externo de configuración de un servidor vsftpd](#)

Sumario

- 1 Instalación del servidor vsftpd
- 2 Notas para la configuración de Acceso Anónimo al servidor FTP
 - ◆ [2.1 Sobre el directorio para usuarios anónimos](#)
 - ◆ [2.2 Solución al error 500 OOPS: vsftpd: refusing to run with writable root inside chroot\(\)](#)
 - ◆ [2.3 Cálculo de los permisos resultantes al usar umask](#)
- 3 Habilitación de cuotas en discos
 - ◆ [3.1 Instalación del paquete quota](#)
 - ◆ [3.2 Edición del sistema de archivos para habilitar cuotas](#)
 - ◆ [3.3 Chequeo del sistema de cuotas](#)
 - ◆ [3.4 Asignación de cuotas a usuarios o grupos](#)
 - ◆ [3.5 Comprobación de cuotas de usuarios](#)
 - ◆ [3.6 Tiempo de Gracia](#)
 - ◆ [3.7 Inicio y paro del servicio de cuotas](#)
- 4 Activación de SSL en FTP
 - ◆ [4.1 Creación del certificado SSL para su uso en el servidor FTP.](#)
 - ◆ [4.2 Modificación del fichero de configuración para activar SSL](#)

Instalación del servidor vsftpd

Para instalar el servidor VSFTPD:

```
apt-get install vsftpd
```

El fichero de configuración del servidor se encuentra en:

```
/etc/vsftpd.conf

# Si se activa el acceso anónimo el directorio por defecto está en:
/srv/ftp

# Por defecto está configurado para que los usuarios anónimos sólo puedan
# descargarse ficheros de ese directorio.
```

Notas para la configuración de Acceso Anónimo al servidor FTP

Sobre el directorio para usuarios anónimos

Si queremos permitir que los usuarios anónimos puedan subir archivos al servidor tendremos que tener en cuenta que:

- El usuario ftp no debe ser propietario del directorio dónde se suban los ficheros.
- El usuario ftp no debe ser miembro del grupo propietario del directorio dónde se suban los ficheros.
- El directorio anónimo debe tener los permisos de escritura correspondientes para OTROS.

```
# En Debian el directorio raíz por defecto del servidor FTP, está situado en:
/srv/ftp

# Y dispone de los siguientes permisos:
drwxr-xr-x 2 root ftp 4096 ene 16 11:41 ftp

# Si se desea configurar un directorio raíz diferente para el servidor anónimo se usa:
anon_root=/directorio

# Por lo tanto si queremos crear un directorio anónimo para escritura el TRUCO está en:
# crear una carpeta por ejemplo llamada pub dentro de /srv/ftp
```

```

mkdir /srv/ftp/pub

# Comprobar que propietario y grupo esté root por ejemplo
chown root.root /srv/ftp/pub

# Y que tenga permisos de RWX en otros para esa carpeta.
chmod 757 /srv/ftp/pub

# No es necesario modificar el anon_root ya que por defecto está puesto a /srv/ftp

# Si queremos que los ficheros que subamos tengan unos permisos por defecto
# deberemos utilizar la opcion chown_upload_mode
# Por defecto está puesta a: -rw----- (0600)
# Ejemplo:
chown_upload_mode=0666

```

Solución al error 500 OOPS: vsftpd: refusing to run with writable root inside chroot()

Este error se da porque vsftpd no permite que los usuarios puedan escribir en su carpeta raíz. Una solución es quitarle los permisos de escritura a esa carpeta. Esto hará que el usuario no pueda hacer nada en su propia carpeta, así que lo mejor es crearle otra dentro con permisos normales para que pueda utilizarla.

Cálculo de los permisos resultantes al usar umask

```

# Cuando usamos umask el valor resultante de los ficheros o directorios enviados al servidor
# será el siguiente:

# Para ficheros:
  666
- umask
-----
permisos resultantes del fichero

# Para Directorios:
  777
- umask
-----
permisos resultantes del directorio.

#Ejemplo:
umask=021

Permiso de los ficheros = 666 - 021 => 645 -> rw-r--r-x
Permiso de los directorios = 777 - 021 => 756 -> drwxr-xrw-

```

Habilitación de cuotas en discos

Instalación del paquete quota

Vsftpd tiene la posibilidad de establecer cuotas de disco para los usuarios del servicio, siendo necesarias gestionarlal desde el sistema operativo, y requiriendo la instalación del paquete **quota**.

```
apt-get install quota
```

Edición del sistema de archivos para habilitar cuotas

En GNU/Linux antes de poder gestionarlal 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. Lo haremos a continuación de **ext3**, por ejemplo:

```

# Editamos el archivo /etc/fstab:
nano /etc/fstab

# Añadimos 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

```

```
#o también nos puede aparecer en lugar de /dev/hda1 el UUID del disco:
UUID=e7b309....90d1-b5a3104130f4 / ext3 usrquota,grpquota,errors=remount-ro 0 1
```

Para que este cambio se haga efectivo, es necesario reiniciar el equipo o volver a montar el sistema de ficheros afectados mediante la orden:

```
mount -o remount /
```

Chequeo del sistema de cuotas

- Podremos chequear las cuotas en nuestro sistema con:

```
quotacheck -augmv
```

Si obtenemos un mensaje del estilo:

Your kernel probably supports journaled quota but you are not using it. Consider switching to journaled quota to avoid running quotacheck after an unclean shutdown.

Tendremos que hacer un cambio en el sistema de cuotas para indicar que se adapte al journaling. Editamos el fichero `/etc/fstab` y escribiremos lo siguiente:

```
UUID=e7b309....130f4 / ext3 usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0 0 0
```

Reiniciamos el sistema y automáticamente se crearán los ficheros `/aquota.user` y `/aquota.group`. En el caso de que fuera necesario crear los ficheros de cuotas (**`aquota.user`** y **`aquota.group`**) se haría mediante la orden:

```
touch PuntoDeMontaje/aquota.user PuntoDeMontaje/aquota.group

# Por ejemplo:
touch /aquota.user /aquota.group

# Y se establecerían los permisos de lectura y escritura solamente (propietario-grupo root):
chmod 600 /aquota*
```

Asignación de cuotas a usuarios o grupos

A la hora de asignar cuotas, tienes varias opciones para imponer límites en el espacio de disco que un usuario o grupo puede ocupar, y cuántos ficheros pueden crear. Puedes limitar el uso de disco basándote en el **espacio en disco (cuotas de bloque)** o en el **número de ficheros (cuotas de inodo)** o una combinación de ambas. Cada uno de estos límites a su vez se divide en dos categorías: **límites suaves (soft)** y **límites duros (hard)**.

Los límites suaves (soft), pueden excederse por un período. Este periodo de tiempo recibe el nombre de periodo de gracia o tiempo de gracia, que por defecto es una semana. Si un usuario sobrepasa su período de gracia, el límite suave se convertirá en un límite duro y no se permitirán usos de disco adicionales. Cuando el usuario devuelve su cuota de uso de recursos a un punto por debajo de su límite suave, el período de gracia se reinicia al valor por defecto del sistema.

Un límite duro (hard) especifica el límite absoluto, que no puede ser excedido nunca. Una vez que un usuario alcanza su límite duro no puede realizar más ubicaciones en el sistema de ficheros en cuestión. Por ejemplo, si el usuario tiene un límite duro de 500 kbytes en un sistema de ficheros y está utilizando 490 kbytes, el usuario solo puede ocupar otros 10 kbytes. Un intento de ocupar 11 kbytes más fallará.

La asignación de cuotas se puede realizar con dos comandos **setquota** o **edquota**:

```
# Ejemplo de asignación de cuota con setquota:
setquota -u usuario 1024 2048 0 0 /dev/sda1

# 1024 indica que el usuario tiene 1024 bloques en nuestro sistema, si sobrepasa ese límite
# obtendrá un mensaje de warning desde el sistema. Si el usuario usa más de 2048 bloques
# no se le permitirá escribir más en el disco.
# Los dos últimos valores a 0 indican que no hay límite en los inodos (ficheros) para soft y hard.

edquota -u NombreUsuario
#o
edquota -g NombreGrupo
```

dependiendo si se establece para un usuario o grupo de ellos. Al ejecutarlo se abrirá el editor establecido por defecto para que se puedan establecer los siguientes parámetros:

- **Blocks:** indica el número de bloques utilizados por el usuario en Kb.
- **Soft:** expresado en Kb, indica el máximo de espacio en disco que la cuota de usuario puede utilizar en esa partición antes de recibir una advertencia, la cual puede superar en un período conocido como de gracia. Pasado es tiempo de gracia el valor soft funciona como si fuera un límite absoluto (hard).
- **Hard:** expresado en Kb, indica el límite absoluto de espacio en disco que nunca podrá superar el usuario.
- **Inodes:** indica el número de ficheros que puede utilizar el usuario.

Comprobación de cuotas de usuarios

```
# Para listar las cuotas de los usuarios:
quota -u idusuario

# o para ver un informe de todas las cuotas:
repquota -a
```

Tiempo de Gracia

En los ejemplos anteriores el factor límite venía indicado por limit. Pero también podemos decidir que un usuario tenga un cierto tiempo para hacer limpieza de su carpeta y recuperar la cuota excedida. Si activamos este sistema el valor Soft será el que se vigile.

Este tiempo se denomina **tiempo de gracia** (por defecto está activado a 6 días). Este tiempo de gracia se puede ajustar para cada usuario individual o para todos los usuarios globalmente:

```
# Para ajustar el tiempo de gracia en segundos (120 en este caso), para un usuario en particular:
setquota -u lucia -T 120 unset /dev/sda1

# Ajusta el tiempo de gracia en el dispositivo /dev/sda1 para todos los usuarios. El tiempo está expresado
# en segundos 86400 (1 día).
setquota -u -t 86400 0 /dev/sda1
```

Inicio y paro del servicio de cuotas

```
# Para iniciar el servicio de cuotas hay que ejecutar la orden:
quotaon -vaug

# y para detenerlo mediante la orden:
quotaoff -vaug
```

Activación de SSL en FTP

Creación del certificado SSL para su uso en el servidor FTP.

```
# Antes de crear el certificado, se recomienda tener actualizado el sistema:
apt-get update
apt-get upgrade
reboot

# Para crear un certificado llamado vsftpd.pem en el directorio /etc/ssl/private/:
# Cubrir todos los datos del certificado correctamente:
openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

# Fijarse que la instrucción termina con /etc/ssl/private/vsftpd.pem
```

Modificación del fichero de configuración para activar SSL

Si no usamos SSL para la autenticación FTP nuestro usuario y contraseña podría ser capturado por un sniffer. Una forma de proteger esa comunicación es activando la comunicación SSL con el servidor FTP y el cliente. Veamos cómo se hace:

```
# Modificaremos el fichero de configuración /etc/vsftpd.conf:
nano /etc/vsftpd.conf

# Ejemplo de fichero de configuración:
```

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=NO
force_local_logins_ssl=NO
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

# Reiniciaremos el servicio:
service vsftpd restart

# Para probar la conexión SSL, nos conectaremos usando un un usuario registrado
# y con un cliente FTP como puede ser Filezilla, y empleando FTP using Explicit SSL.

# Nota en caso de error en la conexión SSL desde Filezilla, añadir el siguiente parámetro:
ssl_ciphers=AES128-SHA

# Reiniciar el servicio vsftpd y probar de nuevo.
service vsftpd restart
```

--Veiga (discusión) 11:23 16 ene 2013 (CET)