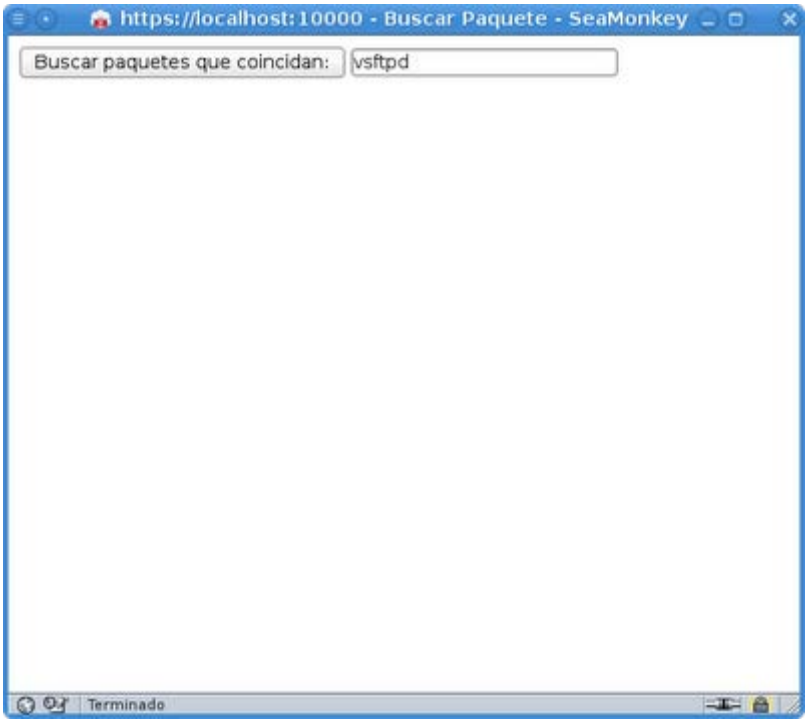
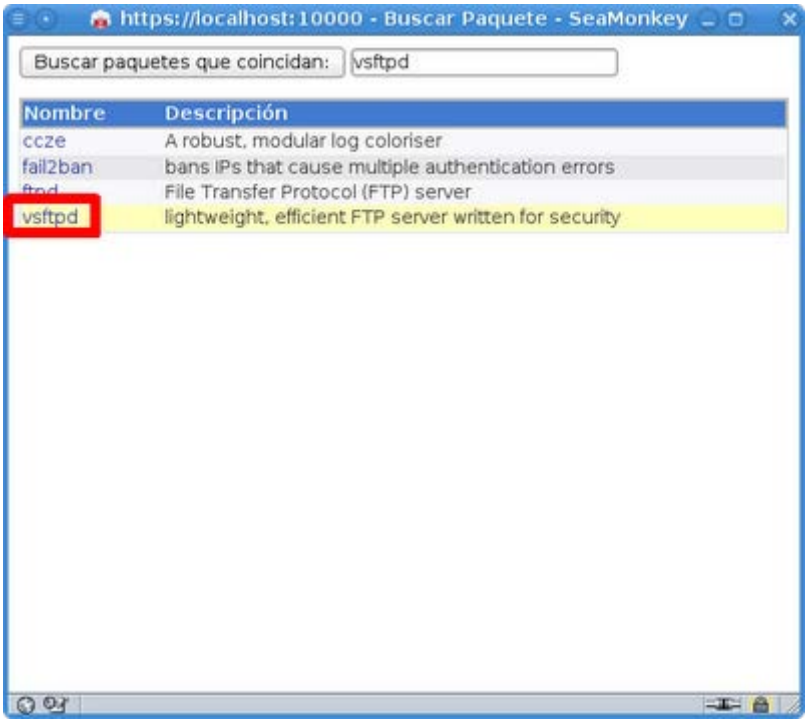
Instalar VSFTPD desde webmin.

Nos vamos a **Sistema > Paquetes de Software**, en el apartado Instalar nuevo paquete, nosotros elegimos la opción **Paquete desde APT**, Pulsamos en **Buscar**

En el buscador de paquetes escribimos VSFTPD

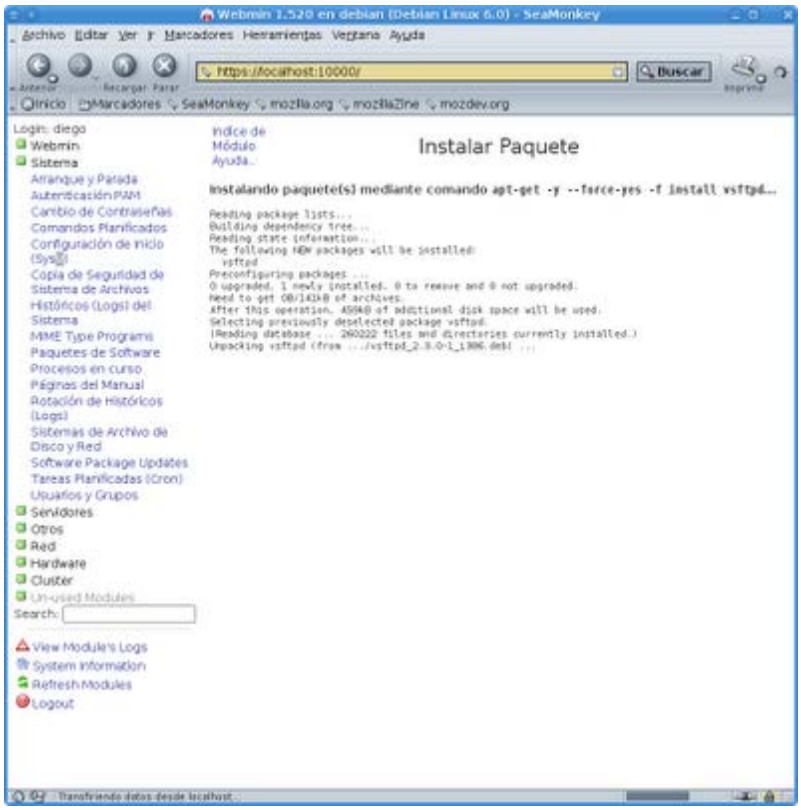


Y al pulsar en **Buscar paquetes que coincidan**: nos muestra el resultado de la búsqueda, en el cual nosotros pinchamos en vsftpd

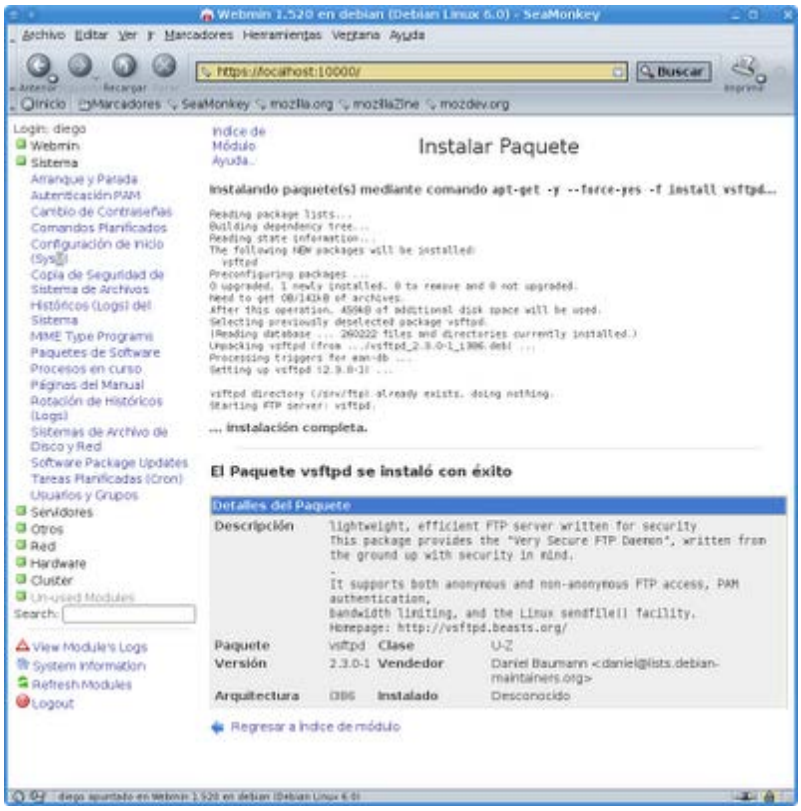


Nos devuelve a la pagina anterior en la cual hemos de pinchar en **Instalar**

Al pulsar en instalar comienza el proceso de instalación.



Hasta que finaliza el proceso de instalación y leemos que vsftpd se instaló con exito.



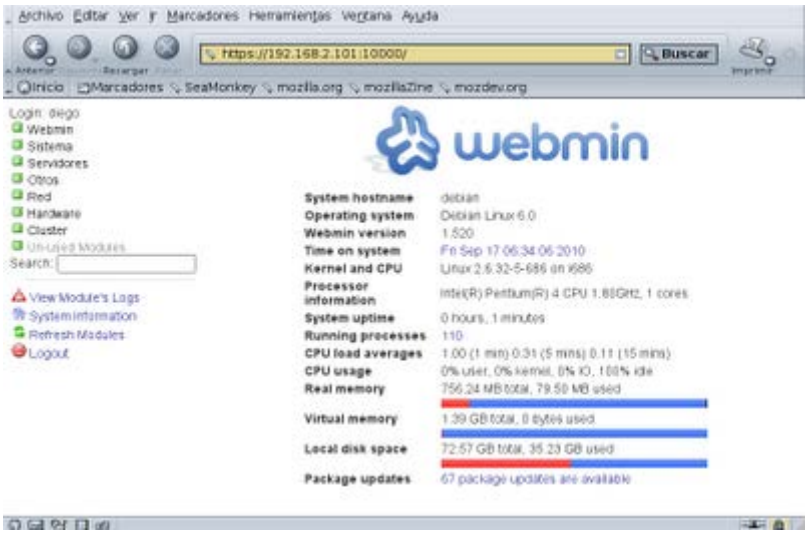
Configurar VSFTPD (Very Secure FTP Daemon)

Entramos en webmin, para ello lanzamos un navegador web y nos dirigimos a cualquiera de las siguientes direcciones:

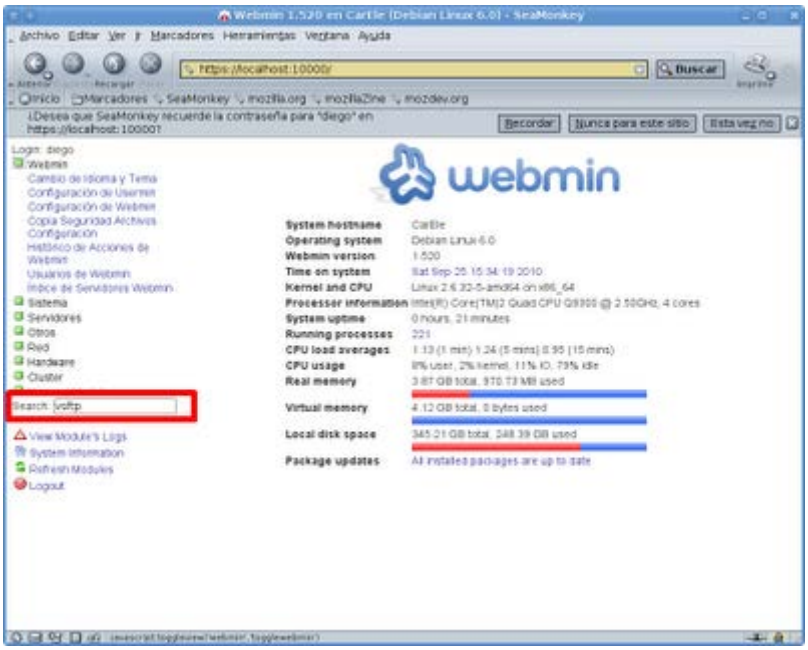
https://localhost:10000
https://127.0.0.1:10000

E introducimos los datos del los campos Username y Pasword para poder entrar.

La primera pantalla nos informa del hardware y los recursos que incluye el ordenador que estamos usando para la gestión y configuración.



Nos dirigimos a la pestaña **Servidores**, en caso de no encontrar el módulo de vsftpd, nos dirigimos a **Un-used Modules**, en este apartado se encuentran una selección de módulos instalados actualmente en webmin sin estar configurados y casi con total seguridad no se encuentran instalados en dicho ordenador. Por ultimo para asegurar mejor que el módulo no se encuentra instalado, puedes usar el buscador para encontrar el módulo

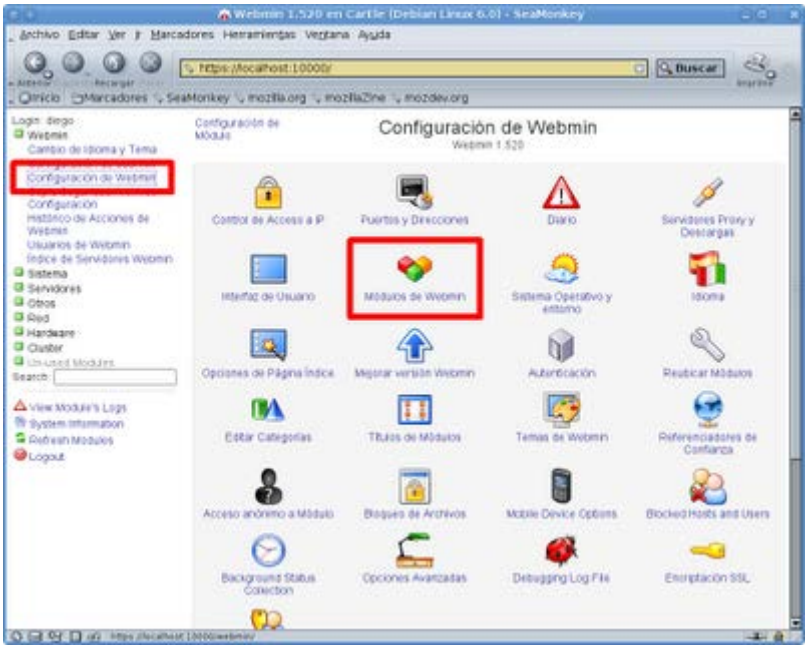


En el caso de vsftpd no se encuentra en ninguna de las dos opciones anteriores, esto no quiere decir que no se pueda usar en webmin, simplemente nos indica que dicho módulo no se instala por defecto en webmin.
Para instalar el módulo vsftpd nos dirigimos a la web oficial de webmin:
http://www.webmin.com
y nos dirigimos a la siguiente pestaña **Third-Party Modules.**

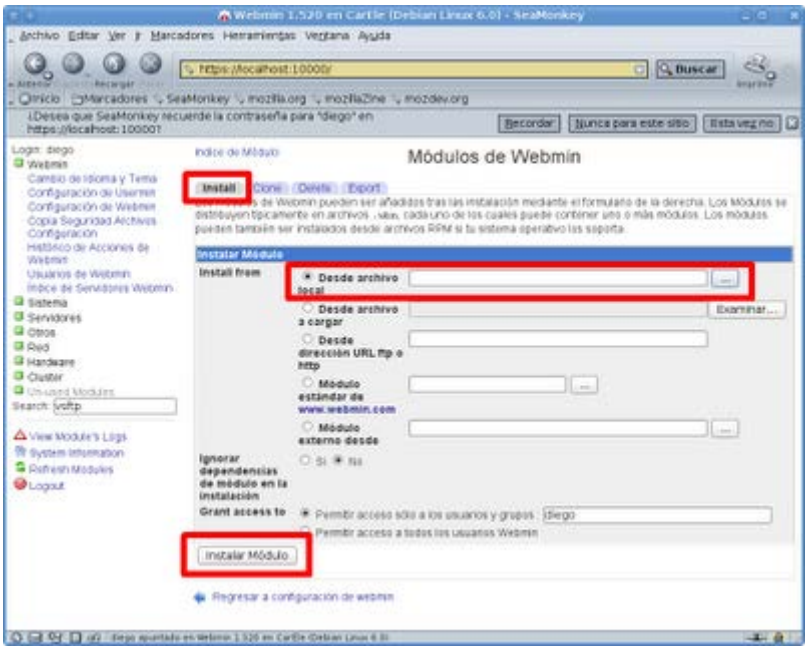
Y en el apartado **Find modules or themes matching** (buscar módulos o temas), ponemos el nombre del módulo que necesitamos instalar, en nuestro caso es vsftp y pulsamos en **Search** (buscar)

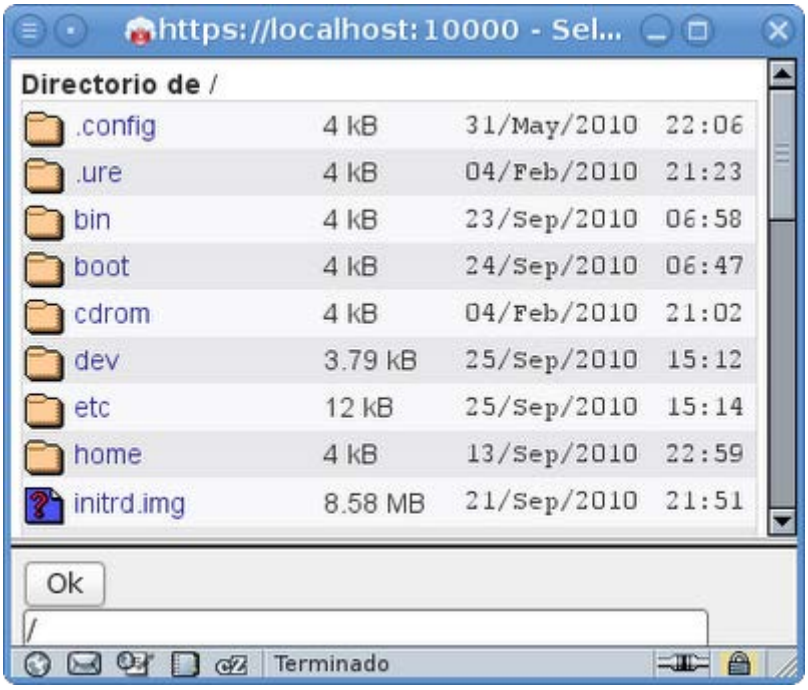
Nos devuelve el siguiente resultado informándonos que el nombre del módulo es **VSFTPD**, y todas las versiones existentes, nosotros elegiremos la ultima versión existente en el momento de realizar este manual **VSFTPD 1.4**, nos bajamos el fichero comprimido pinchando en el enlace **Download** de dicha versión.

Una vez descargado el módulo procedemos a su instalación. Para ello regresamos a **Webmin > Configuración de Webmin > Módulos de Webmin**

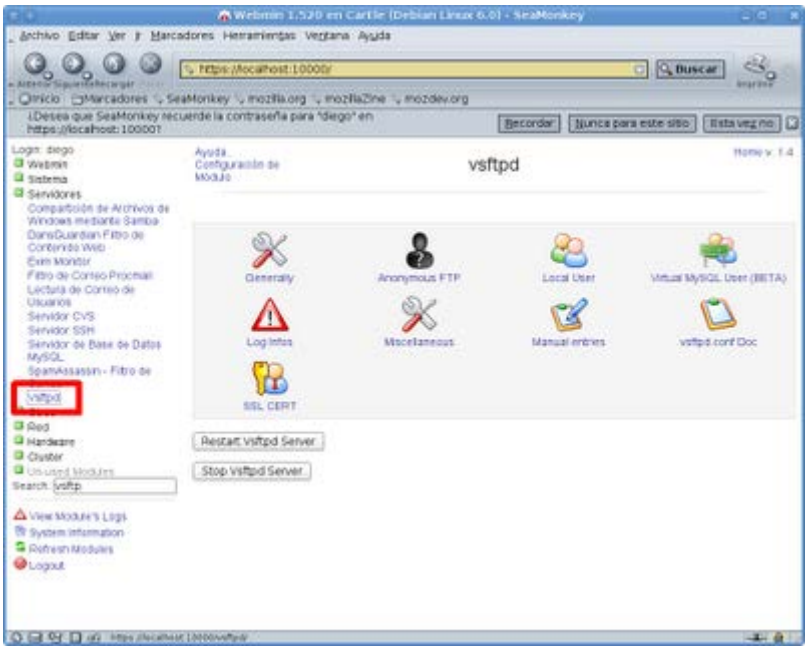


De la cuatro opciones que tenemos en Módulos de Webmin (Instalar, Clonar, Borrar y Exportar), seleccionamos **instalar (Install)** y en este manual vamos a instalar desde el archivo local que nos bajamos antes **vsftpd.tar.gz**, para ello pulsamos en los puntos **(...)** para navegar por nuestro ordenador hasta dar con la del fichero que descargamos antes para su instalación y finalmente pulsamos en **Instalar Módulos**.



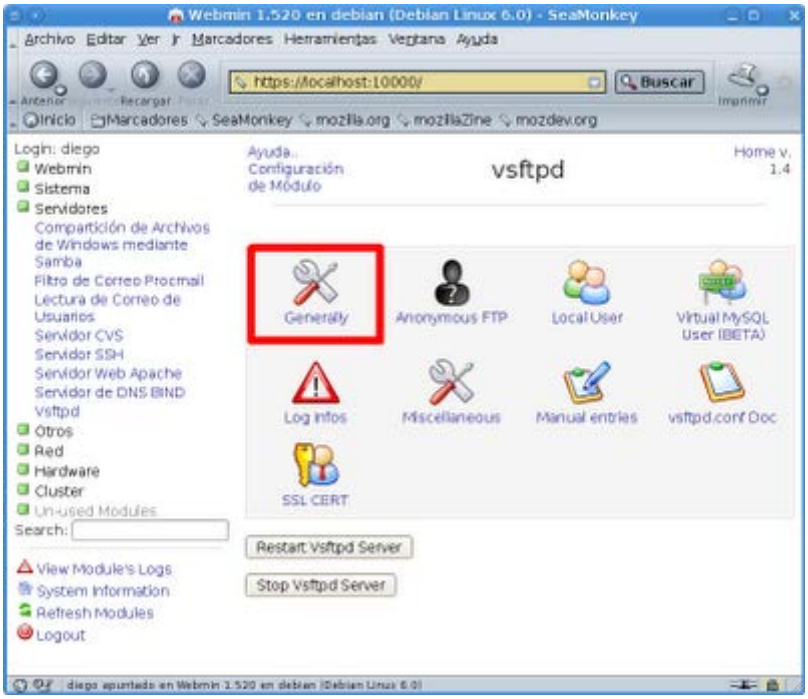


Con esto ya tenemos el módulo cargado en el apartado de **Servidores**



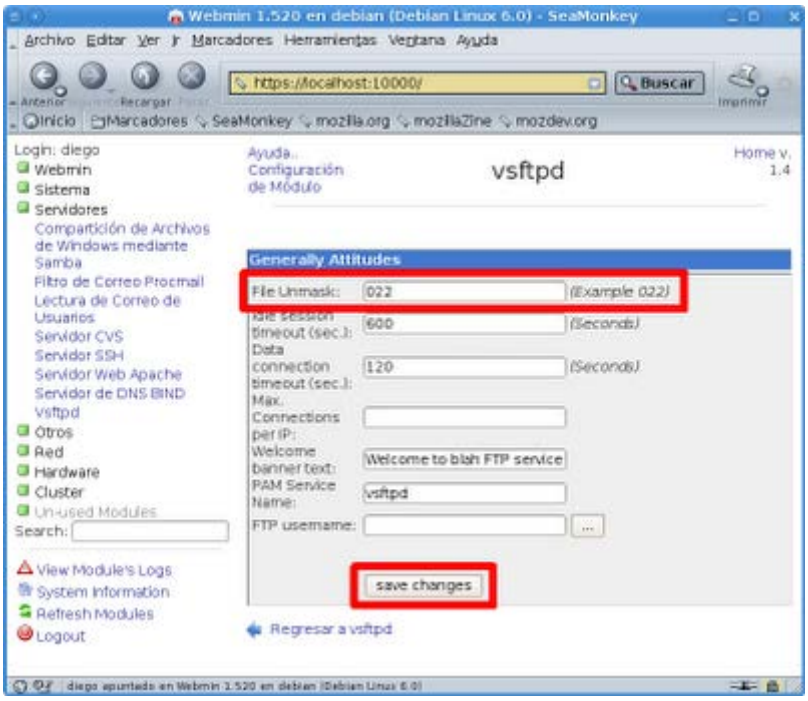
Configuración del entorno FTP

Primero nos dirigimos a **Generally** para configurar el entorno de nuestro servidor FTP

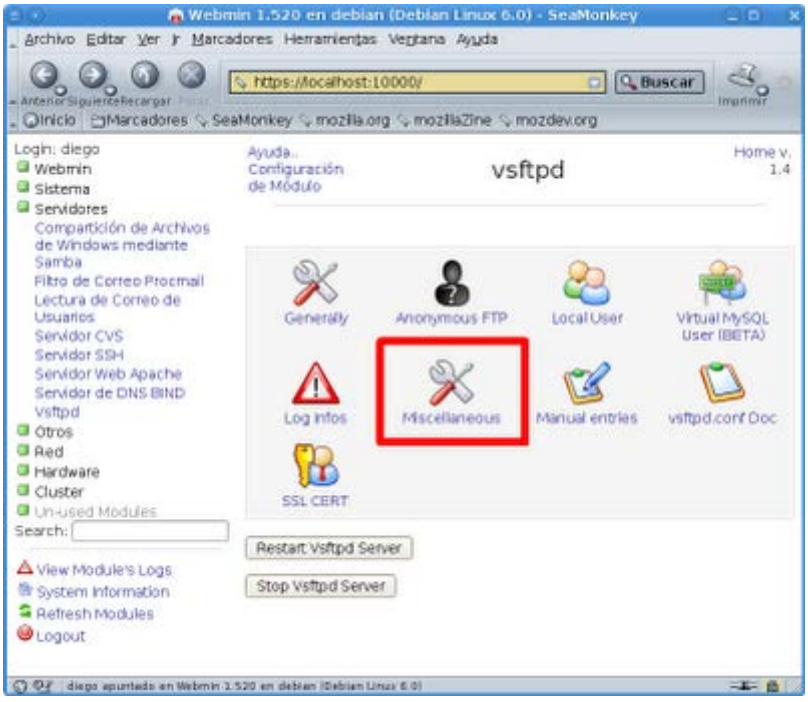


Seleccionamos **Unmak**, para darles los permisos a los ficheros que subamos al servidor, por defecto es 022 pero podemos usar el que mas nos interese. El resto de opciones las podemos dejar por defecto.

Pulsamos en **Save changes** para guardar los cambios realizados.



Seguimos configurando el entorno de nuestro servidor FTP, nos dirigimos a **Miscellaneous**

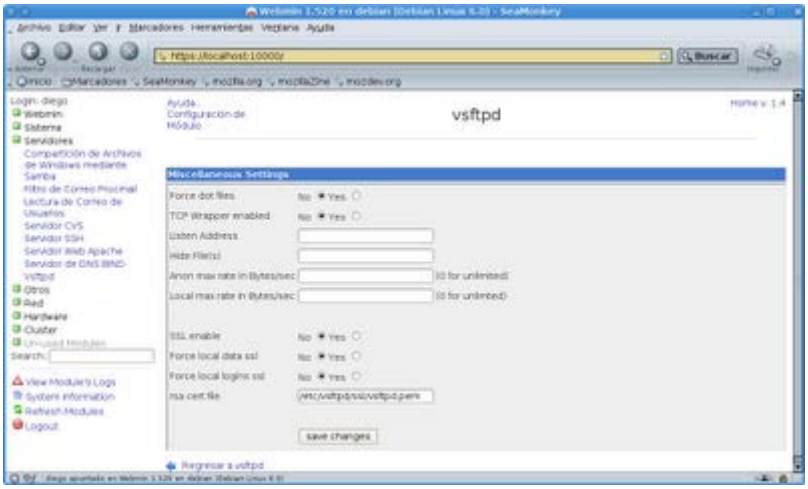


Las opciones que podemos configurar son las siguientes:

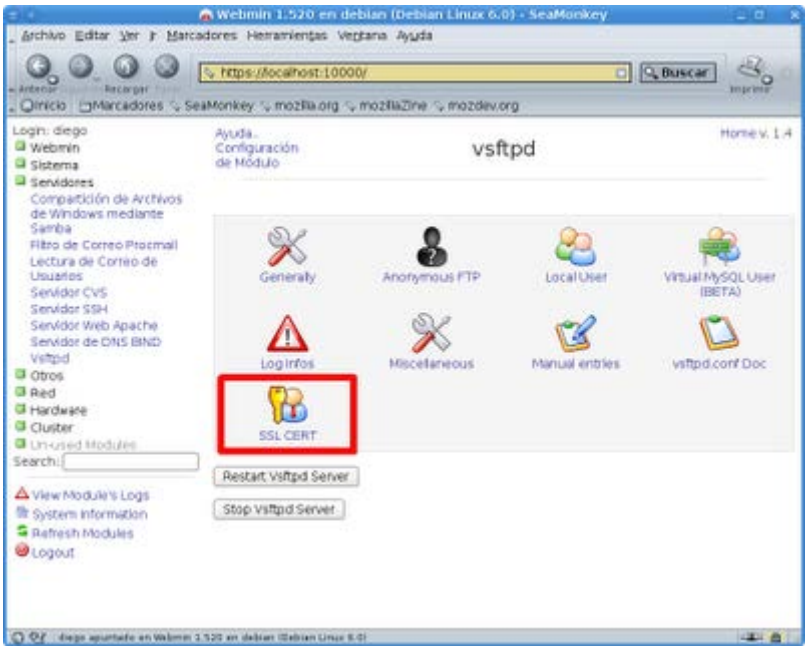
- **Force dot files**: es para que podamos visualizar u ocultar los ficheros ocultos (aquellos que comienzan con un punto)

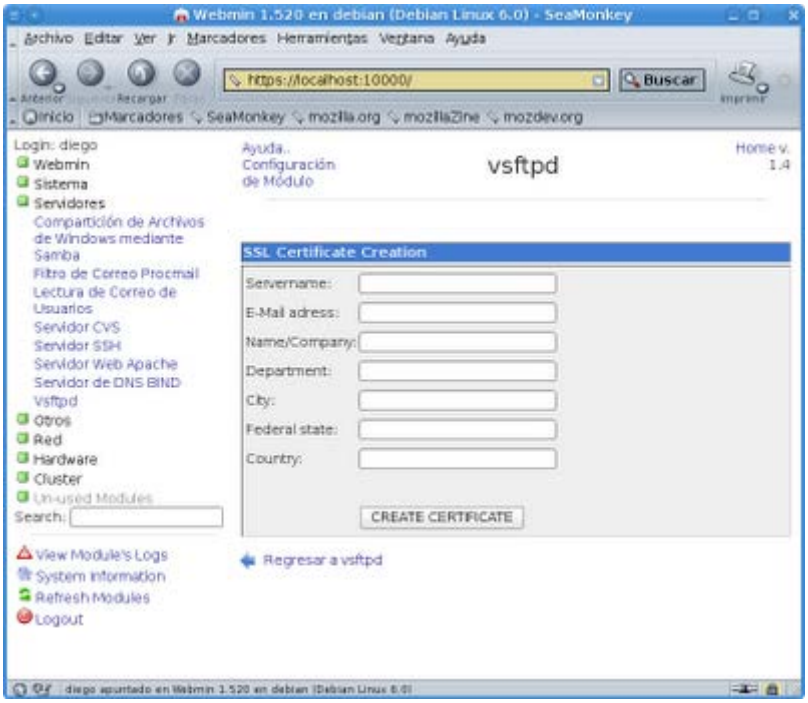
- **TCP Wrapper enabled**: se utilizan para otorgar acceso al servidor si el servidor está configurado en múltiples direcciones IP, se puede utilizar para cargar diferentes archivos de configuración en la dirección IP solicitada por el cliente
- **Listen Address**: Especifica la dirección IP en la cual VSFTP escucha las conexiones de red
- **Hide File(s)**: es para ocultar ficheros y carpetas
- **Anon max rate in Bytes/sec**: especifica la cantidad máxima de datos transmitidos por usuarios anónimos en bytes por segundo. El valor por defecto es 0, lo que no limita el ratio de transferencia.
- **Local max rate in Bytes/sec**: especifica el máximo ratio de transferencia de datos para los usuarios locales conectados en el servidor en bytes de segundo. El valor por defecto es 0, lo que no limita el ratio de transferencia.
- **SSL enable**: permitir SSL (Secure Sockets Layer - Protocolo de Capa de Conexión Segura)
- **Force local data ssl**: Forzar ssl, seguridad local de datos
- **Force local logins ssl**: Obliga a los usuarios a logearse usando ssl
- **rsa cert file**: ruta al fichero del certificado de seguridad

Configuramos las opciones según nuestras necesidades, en este manual solo hemos la opcion Hide Files(s) en la cual hemos puesto un punto (.) para que no muestren los ficheros ocultos.
Pulsamos en **Save changes** para guardar los cambios realizados.



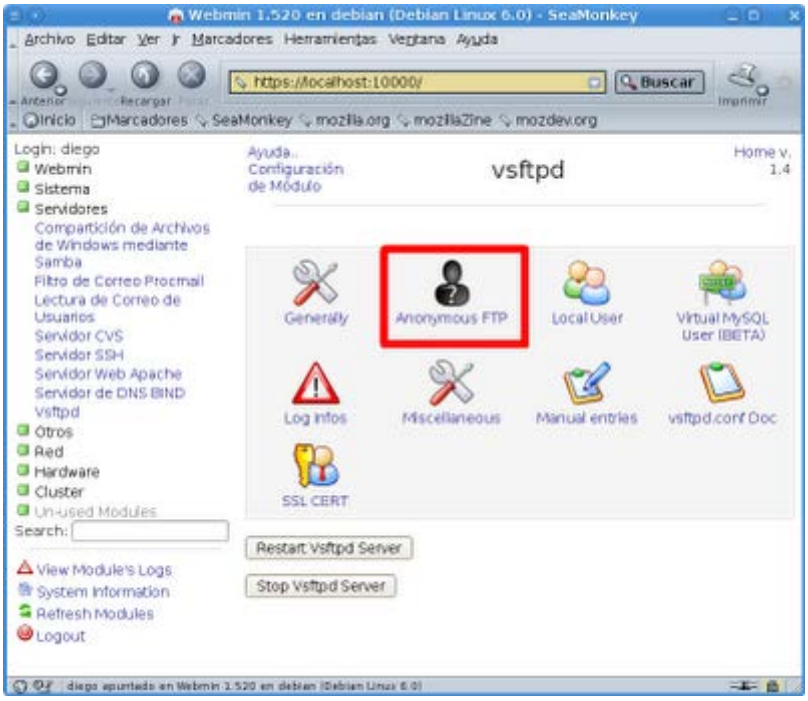
Por ultimo nos quedaría por configurar Secure Sockets Layer (Protocolo de Capa de Conexión Segura), como en este manual no vamos a ser uso de dicho protocolo no lo configuramos.
Pero si mostramos las opciones de configuración que incluye.





Configurar los Usuarios Anónimos y Locales del servidor FTP

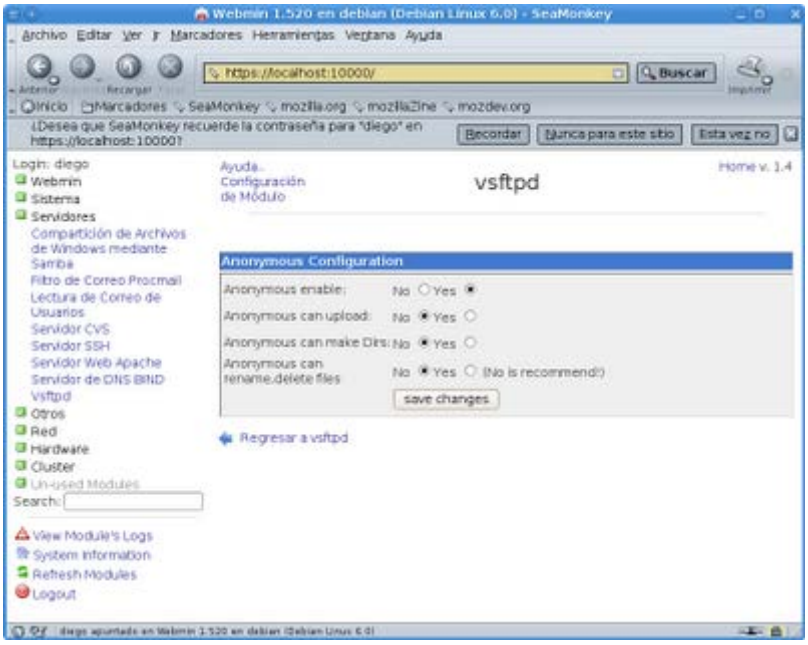
Ahora nos dirigimos a **Anonymous FTP** para configurar las opciones del usuario anónimo.



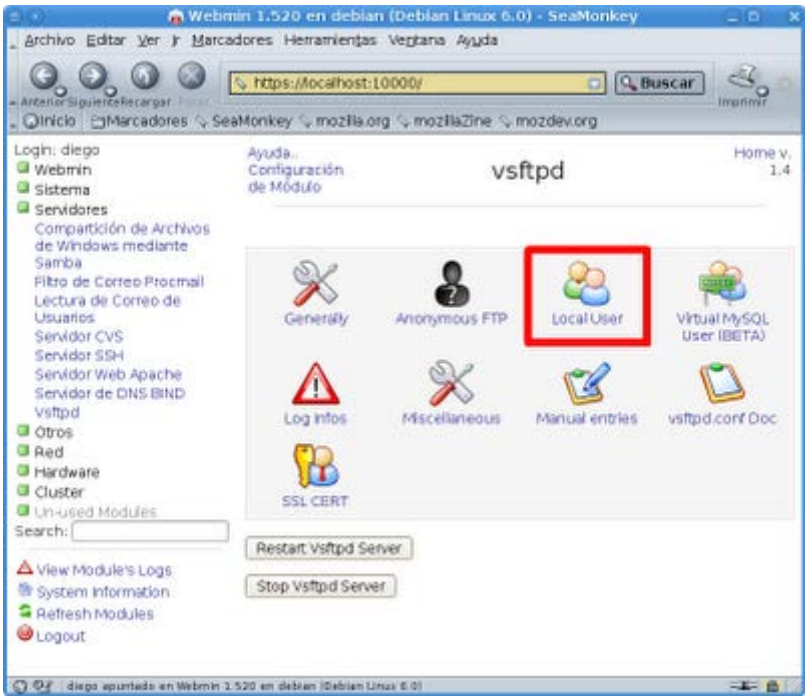
Las opciones son las 4 siguientes:

- **Anonymous enable**: Al estar activada, se permite que los usuarios anónimos se conecten. Se aceptan los nombres de usuario anonymous y ftp
- **Anonymous can upload**: El usuario anónimo puede subir ficheros al servidor.
- **Anonymous can make Dirs**: El usuario anónimo puede crear directorios.
- **Anonymous can rename,delete files**: El usuario anónimo puede renombrar y borrar archivos y carpetas.

Cada uno ha de configurar el servidor de acuerdo a sus necesidades, en este manual necesitamos que el usuario anónimo este activo, pero solo puede descargar ficheros, no puede subir archivos, no puede crear directorios y tampoco puede renombrar o borrar archivos y carpetas.
Pulsamos en **Save changes** para guardar los cambios realizados.



El siguiente paso es configurar los usuarios locales (**Local User**)

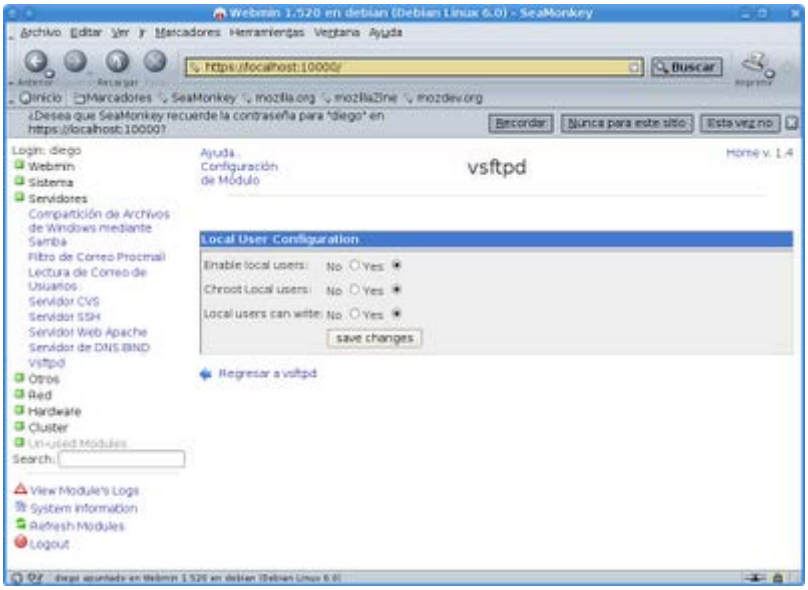


Son 3 las opciones que tenemos para configurar los usuario locales del sistema:

- **Enable local users**: Permitir a los usuarios locales puedan acceder al servidor FTP
- **Chroot Local users**: Restringe a los usuarios locales solo a su directorio de trabajo o le permitimos que pueda navegar por todo el árbol de directorios del sistema.

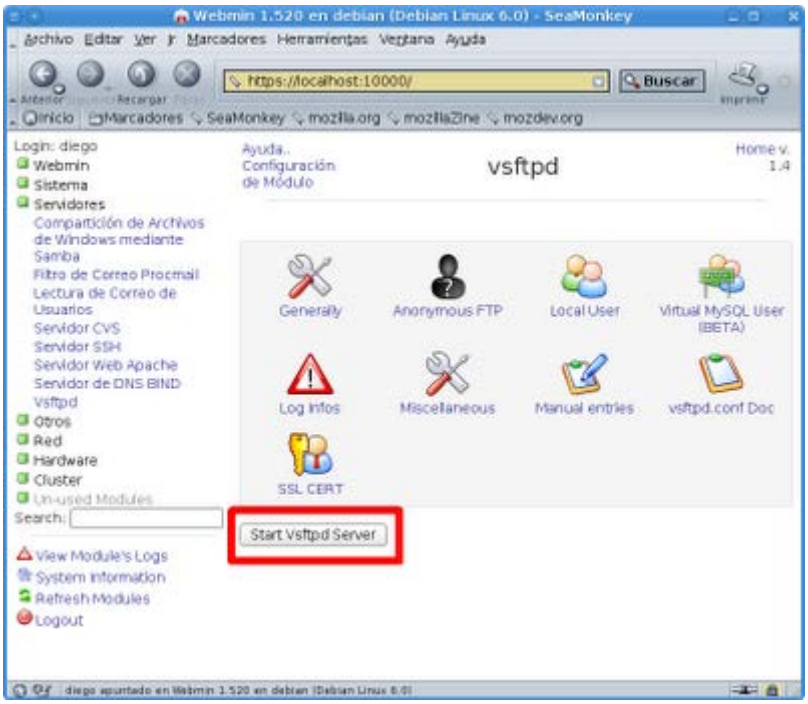
- **Local users can write**: Permitir a los usuario locales puedan escribir (crear archivos y carpetas) en el servidor

Cada uno ha de configurar el servidor de acuerdo a sus necesidades, en este manual necesitamos que los usuario locales puedan acceder al servidor FTP, pueden subir archivos, crear, borrar y renombrar ficheros y carpetas.
Pulsamos en **Save changes** para guardar los cambios realizados.

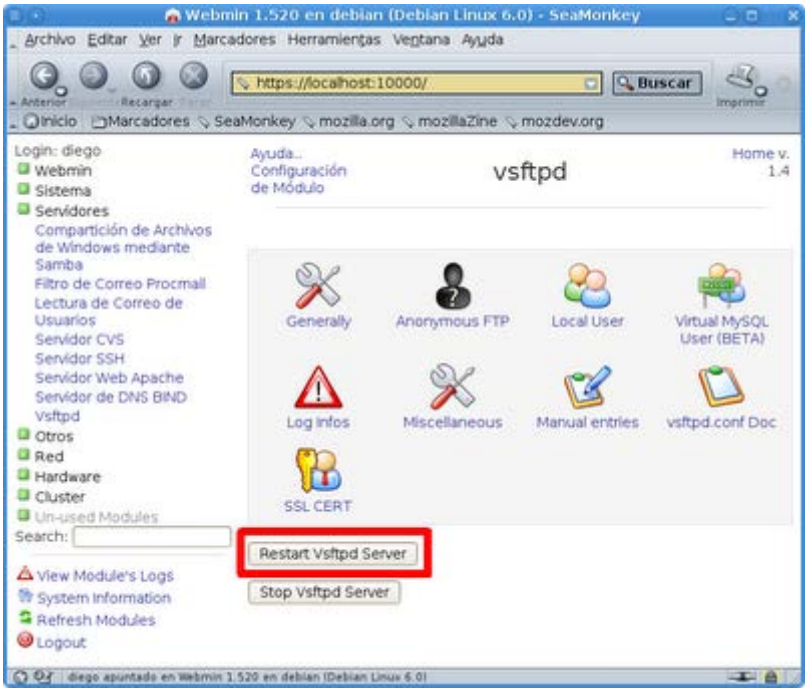


Arrancar o Reiniciar el servidor FTP

Por último y mas importante es arrancar el servidor FTP para que podamos dar servicio. Para ello pulsamos en: **Start Vsftpd Server**



Recordad que cada vez que realicemos una modificación en el servidor, al finalizar los cambios hemos reiniciar el mismo para que estos surtan efectos. Para ello pulsamos en **Restart Vsftpd Server**



Un servicio muy habitual es el ftp, sobre todo si tenemos montado un servidor Web para que los diseñadores y webmasters puedan dejar allí sus creaciones sin molestar a los administradores, nosotros. Con este objetivo, vamos a montar un servidor ftp.

Usuario: client1
Acceso a su directorio: /var/www/dominio1
Sin shell en el sistema y en un entorno chroot

Usuario: client2
Acceso a su directorio: /var/www/dominio2
Sin shell en el sistema y en un entorno chroot

Usuario: webmaster
Acceso a su directorio: /var/www
Sin shell en el sistema y en un entorno chroot

Preparación del sistema

Antes de instalar el servidor ftp vamos a crear los usuarios y securizarlos para que tengan los mínimos permisos y sólo puedan hacer lo que nosotros definamos.

Crearemos un grupo llamado ftp al cual asociaremos los usuarios (NO HACE FALTA PORQUE YA EXISTE).

```
# groupadd ftp
```

Creamos los usuarios con sus correspondientes características.

```
#useradd -g ftp -d /var/www/dominio1 -c " Cliente 1 " client1
#useradd -g ftp -d /var/www/dominio2 -c " Cliente 2 " client2
#useradd -g ftp -d /var/www -c " webmaster " webmaster
```

Les asignamos un password a los usuarios con el comando passwd. Si no tiene password no funcionará.

Ahora creamos una shell fantasma en el directorio correspondiente.

```
#mkdir /bin/ftp
```
(TAMPOCO ES NECESARIO YA QUE ESISTE /bin/false)

Editamos el fichero /etc/shells y la añadimos en la ultima línea y continuación editamos el fichero /etc/passwd y buscamos las líneas donde están definidos los usuarios que hemos creado antes y les añadimos el shell falso:

```
client1:x:1005:1005: Cliente 1 :/var/www/dominio1:/bin/ftp
client2:x:1006:1005: Cliente 2 :/var/www/dominio2:/bin/ftp
webmaster:x:1007:1005: webmaster :/var/www:/bin/ftp
```

Configuración del servidor

El fichero de configuración del servidor se encuentra en /etc/vsftpd.conf. Lo editamos para configurarlo a nuestro gusto y objetivo. El contenido es algo parecido, buscamos las líneas indicadas y las modificamos:

```
# Example config file /etc/vsftpd.conf
#Escuchando
listen=YES
#
.....................................
# Desactivamos el acceso anónimo
anonymous_enable=NO
#
# Descomentamos la línea para que se puedan conectar
local_enable=YES
#
# Permitimos a usuarios locales escribir
write_enable=YES
#
# APLICA CONFIGURACIÓN UMASK
local_umask=003
#Mensajes welcome
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
.....................
#
# You may override where the log file goes if you like. The default is shown
# below.
xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format
xferlog_std_format=YES
# Se descomenta esto para crear una jaula
chroot_local_user=YES
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
#chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
#
# Debian customization
# secure_chroot_dir=/var/run/vsftpd
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
# This option specifies the location of the RSA certificate to use for SSL
```

```
# encrypted connections.
#rsa_cert_file=/etc/ssl/certs/vsftpd.pem
```

NO SE PARA QUE LO PONE SI LUEGO NO DA LISTA DE USUARIOS PARA QUE TENGAN ACCESO, CREO QUE NO HACE FALTA, ADEMÁS ESTÁ MEZCLANDO EL ENJAULAR USUARIOS CON EL ACCESO DE LOS USUARIOS

```
userlist_enable=YES
tcp_wrappers=YES
userlist_deny=NO
```

A continuación creamos el fichero vsftpd.chroot_list el cual tendrá la lista de usuarios que no tendrán acceso al servidor:

```
# touch /etc/vsftpd.chroot_list
```

Volcamos los datos a este fichero desde /etc/password con el comando.

```
# cat /etc/passwd | awk -F: '{ print $1 }' > /etc/vsftpd.chroot_list
```

Esto nos genera un fichero con los login de usuarios del sistema del cual quitamos los que si queremos que tengan acceso y los ponemos en el fichero /etc/vsftpd.user_list.

Ejemplos de ficheros:

vsftpd.chroot_list

```
# usuarios con no acceso
root
daemon
bin
sys
sync
games
man
lp
mail
news
```

vsftpd.user_list

```
#usuarios con acceso
webmaster
client1
client2
```

Afinando aún más

Dentro del fichero de configuración (vsftpd.conf) algunas opciones interesantes que también podemos controlar son las siguientes:

```
#opciones de transferencia
#ancho banda por usuario anónimo 5kb
anon_max_rate=5100
#ancho de banda por usuario local 5kb
local_max_rate=5100
#número máximo clientes simultáneos
max_clients=5
#máximo conexiones por ip
max_per_ip=2
#envía al sistema
syslog_enable=yes
session_support=yes
```

Usuarios de ftp virtuales con vsftpd y MySQL

Un problema que se me ha presentado más de una vez es dar acceso FTP a determinadas carpetas a usuarios que necesitan actualizar archivos en ellas. Por regla general habría que crear un usuario del sistema que tuviese su "home" en esa carpeta o un enlace simbólico desde otra, pero nunca me ha gustado la idea de crear usuarios a diestro y siniestro, aunque sean sin privilegios. Buscando un día, empecé a encontrar información sobre cómo crear usuarios "**virtuales**" en vsftpd y me gustó mucho la idea, combinando esto con la gestión de usuarios en **MySQL** podría tener un sistema bastante sencillo de dar acceso **FTP** a unos cuantos usuarios sin incrementar los del sistema y, por tanto, sin abrir agujeros de seguridad.

Lo primero será instalar los módulos necesarios, asumiendo que ya tienes el servidor **MySQL** funcionando. Nos hará falta el paquete **vsftpd** y el **pam_mysql** que permitirá hacer autentificaciones contra una base de datos de este tipo.

1. yum install pam_mysql vsftpd

Ahora configuramos el archivo */etc/pam.d/vsftpd* para que quede así;

1. [osus@servidor vsftpd]# cat /etc/pam.d/vsftpd
2. auth required /lib/security/pam_mysql.so user=vsftpd passwd=clave host=localhost db=basedatos table=usuarios usercolumn=usuario passwdcolumn=pass crypt=0

3. account required /lib/security/pam_mysql.so user=vsftpd passwd=clave host=localhost db=basedatos table=usuarios usercolumn=usuario passwdcolumn=pass crypt=0
4. session required /lib/security/pam_mysql.so user=vsftpd passwd=clave host=localhost db=basedatos table=usuarios usercolumn=usuario passwdcolumn=pass crypt=0

Esto indica a **vsftpd** que debe autenticarse contra "*basedatos*" en "*localhost*" con el usuario "*vsftpd*" y la clave "*clave*" y que debe buscar en la tabla "*usuarios*" con las columnas "*usuario*" y "*pass*". Qué evidente es todo .

El último parámetro, "*crypt*", indica el modo en que se guardarán las claves:

- 0 para claves en texto plano sin encriptar
- 1 para claves encriptadas con la función *crypt()*
- 2 para claves generadas con la función *PASSWORD()* de **MySQL**
- 3 para claves en *md5*

Escoge el sistema que prefieras. Dejaremos ahora el archivo de configuración principal de este modo:

1. [osus@servidor vsftpd]# cat /etc/vsftpd/vsftpd.conf
2. ftpd_banner= "Servidor FTP"
3. anonymous_enable=NO
4. chroot_local_user=YES
5. guest_enable=YES
6. guest_username=ftpoculto
7. hide_ids=YES
8. listen=yes
9. listen_address=192.168.3.254
10. listen_port=21
11. local_enable=YES
12. max_clients=100
13. max_per_ip=5
14. pam_service_name=vsftpd
15. use_localtime=YES
16. user_config_dir=/etc/vsftpd/usuarios
17. userlist_enable=YES
18. userlist_file=/etc/vsftpd/denied_users
19. virtual_use_local_privs=YES
20. xferlog_enable=YES
21. async_abor_enable=YES
22. connect_from_port_20=YES
23. dirlist_enable=NO
24. download_enable=NO
25. local_umask=000

Con esto le estamos diciendo que no permitiremos el acceso anónimo y que el usuario real que se utilizará será "*ftpoculto*", los usuarios virtuales se comportarán como este usuario. Le indicamos, además, que busque los usuarios virtuales en */etc/vsftpd/usuarios*

y que no deje entrar a ningún usuario real, sólo a los virtuales. Para esto último haremos lo siguiente:

1. cat /etc/passwd | cut -d ":" -f 1 | sort > /etc/vsftpd/denied_users

Así añadimos a la lista de usuarios denegados a todos los usuarios del sistema, no hay que ponerlos a mano uno a uno .

Ahora debemos configurar el acceso para cada usuario dentro de la carpeta "*usuarios*". El nombre del archivo debe ser el mismo que el del usuario que se ha añadido a la base de datos, el que utilizará el cliente para conectarse. Yo, por ejemplo, suelo utilizar como nombres el dominio del cliente, así se quién es quién.

1. [osus@servidor usuarios]# cat tudominio.com
2. dirlist_enable=YES
3. download_enable=YES
4. local_root=/var/www/tudominio.com/
5. write_enable=YES
6. anon_world_readable_only=NO

Tendremos que configurar el directorio de este usuario para que pueda escribir en él. Para conseguirlo recordamos que **vsftpd** utilizaría el usuario real "*ftpoculto*". Debemos, por tanto, dar permisos sobre los directorios de los usuarios virtuales a ese usuario:

1. chown -R ftpoculto.users /var/www/tudominio.com

Con esto, el usuario "*tudominio.com*" podrá moverse en */var/www/tudominio.com* a sus anchas .

La verdad es que me ha funcionado muy bien siempre. Si se combina con un sistema de acceso VPN sencillo, de manera que el puerto **FTP** no tenga que estar abierto púclibamente, queda todo muy robusto y seguro además de que es muy sencillo añadir nuevos usuarios, incluso lo puedes automatizar con un *script* ya que solamente hay que añadir un registro en la base de datos y crear el archivo de configuración en */etc/vsftpd/usuarios*.

Es una buena idea en pequeños entornos ISP no dedicados o especializados, entornos donde los usuarios no van a necesitar habitualmente acceso FTP (cms, blogs, webs corporativas…).

Hay muchos más parámetros en **vsftpd**, desde limitar el ancho de banda por usuario hasta utilizar **SSL** en las conexiones, sólo hay que leer un poco la documentación