

Instalación del paquete del servidor vsftpd

La manera más sencilla de hacerlo consiste en dirigirse a *Sistema*, seleccionar *Administración* y pasar a *Gestor de paquetes Synaptic*. Una vez allí, se buscan los paquetes *vsftpd* y *maracr* para su instalación, y pulsamos *Aplicar*.

También puede realizarse la operación a través de la línea de comandos. Basta con acceder como usuario administrador (*sudo*) y ejecutar la instalación del paquete *.deb*:

```
$sudo apt-get install vsftpd
```

De este modo, se crea el nuevo usuario *ftp* en el sistema, y es incluido en el grupo *nogroup*.

El directorio home del usuario *ftp* (**/home/ftp**) pertenece a *root* y al grupo *nogroup*. Allí se alojan los archivos que comparte el servidor FTP para los usuarios anónimos.

Características principales del servidor vsftpd

- **Asigna permisos mínimos:** al lanzarlo, se ejecuta un proceso llamado «padre» con unos permisos básicos. En la medida en que llegan conexiones entrantes (peticiones de clientes FTP), el proceso padre crea nuevos procesos «hijos» —cada uno de los cuales atiende a una conexión— con los permisos mínimos para llevar a cabo la tarea.
- **Utiliza el entorno chroot:** estos procesos hijos se ejecutan en lo que se conoce como una «jaula chroot», en el que se toma como directorio raíz el directorio compartido (donde se encuentran los archivos disponibles vía FTP). Si, por ejemplo, el directorio compartido es **/home/ftp/**, gracias a *chroot* se convierte en el directorio raíz.

El servidor *vsftpd* basa su seguridad en estas dos características fundamentales. Si los procesos que atienden las peticiones FTP tienen unos permisos mínimos y solo pueden acceder al directorio compartido, un hipotético atacante únicamente podría acceder a los archivos del directorio compartido.

Al instalar el paquete de *vsftpd* se crean en el sistema los siguientes archivos y directorios:

Archivo/Directorio	Descripción
/etc/init.d/vsftpd	Archivo que inicia el servicio.
/usr/sbin/vsftpd	Archivo ejecutable.
/etc/vsftpd.conf	Archivo de configuración de <i>vsftpd</i> .
/home/ftp/	Directorio que contiene los archivos que comparte el servidor FTP.
/etc/ftpusers	Contiene la lista de usuarios que no se podrán conectar al servicio FTP.

Tabla CD 5.1. Archivos de *vsftpd*.

Configuración de vsftpd

Todas las opciones de configuración se encuentran en el archivo `/etc/vsftpd.conf`. La estructura de las líneas es siempre la siguiente:

```
Directiva=valor
```

`Directiva` es el nombre de la propiedad que se configurará y a la que se le asigna el valor correspondiente. No debe haber espacios antes y después del símbolo «=» (igual), ya que de lo contrario la directiva tendrá un valor nulo.

Las opciones en cuestión pueden ser numéricas, de cadena o bien booleanas, en cuyo caso el campo `valor` podría contener `YES` o `NO`.

Secciones del archivo de configuración

1. Ejecución del servidor

El servidor `vsftpd` puede ejecutarse como proceso independiente (standalone). Para ello, hay que activar la directiva siguiente:

```
listen=YES
```

Al hacerlo, es preciso asegurarse de que la directiva `listen_ipv6` está desactivada, ya que esta atiende peticiones solo para sockets `ipv6`.

2. Gestión de usuarios

No es preciso que los usuarios tengan una cuenta en el sistema, ya que por defecto es posible conectarse de manera anónima. Las siguientes líneas establecen los tipos de usuario a los que se permite el acceso:

```
anonymous_enable=YES
```

```
local_enable=YES
```

La primera línea indica que cualquier usuario se puede conectar (`YES`) al servidor dando el nombre de `anonymous` o `ftp`. Como contraseña, bastará una cuenta de correo¹.

La segunda indica que los usuarios locales pueden conectarse al servidor (`YES`). En el caso de que se desee impedirlo, bastará con cambiar el valor (`NO`) o comentar la línea con el signo «#» (almohadilla).

3. Descarga de archivos

Cuando un usuario anónimo se conecta al servidor FTP, entra en el directorio `home` del usuario `ftp` (`/home/ftp`) y lo convierte en su directorio raíz mediante la jaula `chroot`. Según los permisos asignados, podrán descargarse los archivos que existan en él.

Cuando un usuario local se conecta, hay dos opciones:

1. Se conecta como usuario del sistema, en cuyo caso el directorio `home` será el que posee como usuario del sistema (`/home/nombre_usuario`). El directorio raíz será el del sistema completo. Este usuario podrá descargarse archivos de *todo* el sistema en función de los permisos asignados.

¹ Normalmente solo se suele comprobar si existe el símbolo `@`, por lo que la cuenta `a@b.c` puede ser válida, aunque si interesa que se envíe información hay que poner una que se utilice.

5 Servicio FTP

- Se conecta como usuario del sistema pero se le cambia su directorio raíz a su directorio home. En consecuencia, no tiene disponible el resto del sistema de archivos. Para ello tan sólo habrá que activar la directiva siguiente:

```
chroot_local_user=YES
```

En general, habrá que tener activada esta segunda opción para limitar el ámbito de actuación, bajo el servicio FTP, de los usuarios locales.

Si interesa en el sistema que determinados usuarios locales no queden recluidos en su directorio home (es decir, no queden «enjaulados») cuando se conectan al servidor FTP, pueden incluirse los nombres de conexión en un archivo utilizando la directiva siguiente:

```
chroot_list_file=/etc/vsftpd.chroot_lista
```

4. Carga de archivos para usuarios locales

Si se permite que los usuarios locales suban o carguen archivos al servidor FTP, habrá que habilitar la siguiente directiva:

```
write_enable=YES
```

Con esta directiva² se pueden establecer los permisos con los que quedará el archivo subido al servidor FTP:

```
local_umask=022
```

De este modo, se indica que los permisos de los archivos serán 644, es decir, de lectura y escritura para el dueño y solo de lectura para el grupo y los demás usuarios (*r w - r - - r - -*).

Por último, puede habilitarse la carga de archivos en formato ASCII en el servidor. Bastará con la directiva siguiente:

```
ascii_upload_enable=YES
```

5. Carga de archivos para usuarios anónimos

Por defecto la carga de archivos para los usuarios anónimos está desactivada. Para activarla hay que incluir la directiva:

```
anon_upload_enable=YES
```

Se ha de crear un directorio (*incoming*, por ejemplo) con permisos suficientes para que puedan escribir en él los usuarios.

```
$sudo mkdir /home/ftp/incoming
```

```
$sudo chmod 777 /home/ftp/incoming
```

Por defecto, los archivos cargados lo harán con permisos 600. Si se quiere que un usuario anónimo pueda descargarlos, habrá que cambiarlos a 644. Para ello, deberemos incluir la directiva:

```
anon_umask=022
```

En el caso de que se quiera permitir que los usuarios anónimos modifiquen los archivos pertenecientes a usuarios anónimos y que puedan crear directorios, habrá que activar estas otras directivas:

```
anon_other_write_enable=YES
```

```
anon_mkdir_write_enable=YES
```

² Se recomienda repasar las órdenes `chmod` y `umask`, así como el esquema de permisos para archivos y directorios utilizado en GNU/Linux.

5 Servicio FTP

6. Visualización de mensajes

Al conectarse un usuario al servicio FTP y hacer un cambio de directorio dentro del directorio raíz de descargas (por ejemplo, *incoming*), puede visualizarse un mensaje cuyo texto se almacena en el archivo **.mensaje**. Para ello habrá que:

Crear el archivo **.mensaje** e incluir el texto que se quiera visualizar.

Añadir las directivas siguientes en el archivo de configuración:

```
dirmessage_enable=YES  
message_file=.mensaje
```

También se puede establecer un mensaje de bienvenida general cuando se conecta el usuario al servidor FTP con esta directiva:

```
ftpd_banner="Bienvenido al Servidor FTP del aulaSER.com"
```

7. Registro de actividad

El registro de actividad se lleva a cabo mediante el archivo **/var/log/vsftpd.log**. Las directivas correspondientes son:

```
xferlog_enable=YES  
xferlog_file=/var/log/vsftpd.log
```

8. Tiempos de conexión

Existen una serie de directivas relacionadas con los tiempos de conexión.

A la hora de establecer la conexión (por defecto, 60 segundos) de un usuario remoto en modo pasivo, se emplea la directiva siguiente:

```
accept_timeout=60
```

En cambio, para indicar el tiempo máximo que el servidor espera cuando una transferencia no progresa (por lo general, 300 segundos), habrá que utilizar esta otra:

```
data_connection_timeout=300
```

En cuanto al tiempo máximo concedido a un usuario remoto que no está activo (es decir, que no está ejecutando órdenes ftp), se establece con la directiva siguiente.

```
idle_session_timeout=300
```

Al igual que en el caso anterior, se asignan por defecto 300 segundos. Pasado este tiempo, se corta la conexión.

9. Listado recursivo

El paquete vsftpd es sencillo y no dispone de muchas opciones con las que moverse por dentro del directorio raíz. Existe una directiva que permite el listado recursivo dentro de un directorio y que puede ser útil. Es la siguiente:

```
ls_recurse_enable=YES
```

Ejecución del servicio vsftpd

Una vez está configurado el servicio, ya se puede lanzar mediante esta orden:

```
$sudo /etc/init.d/vsftpd start
```

Otras opciones disponibles son stop (parar), reload (recarga) y restart (parada e inicio).

A partir de este momento, el servidor FTP atiende peticiones FTP en el puerto 21 TCP.

Para establecer la conexión vía FTP desde la línea de comandos, el usuario debe ejecutar la siguiente orden:

```
$ ftp servidor
```

```
$ ftp 192.168.100.254
```

```
$ ftp ftp.aulaSER.com
```

Configurar el servidor vsftpd para usuarios anónimos

Antes de realizar esta operación, habrá que asegurarse de que se cumplen estos dos requisitos:

1. Se ha instalado en el equipo *servidor* el paquete del servidor FTP vsftpd.
2. Solo se servirán peticiones hechas por usuarios anónimos.

A continuación, habrá que comprobar que el servidor FTP funciona correctamente:

```
$ ftp localhost
```

Se edita el archivo de configuración **/etc/vsftpd.conf** para comprobar que se han activado las directivas que determinan el modo de acceso de los usuarios anónimos al servidor FTP.

Para activar usuarios anónimos:

```
anonymous_enable=YES
```

Para desactivar usuarios locales:

```
local_enable=NO
```

En el caso de que se desee que los usuarios anónimos puedan escribir siempre que los permisos establecidos lo permitan, habrá que indicar los valores siguientes:

```
anon_umask=022
```

```
write_enable=YES
```

Para que los usuarios anónimos puedan crear directorios, habrá que especificarlo de esta manera:

```
anon_mkdir_write_enable=YES
```

Asimismo, para permitir que los usuarios anónimos suban archivos al servidor³ hay que activar:

```
anon_upload_enable=YES
```

A estas directivas hay que añadir las generales de servidor, así como las empleadas para la generación de logs y la visualización de mensajes.

Por último, antes de cerrar el archivo de configuración habrá que eliminar los comentarios de las directivas correspondientes.

³ Debe estar activada la directiva `write_enable=YES`.

Configurar el servidor vsftpd para usuarios del sistema

Como en el caso anterior, antes de empezar conviene asegurarse de que se cumplen estos requisitos:

1. Se ha instalado en el equipo *servidor* el paquete FTP vsftpd.
2. Solo se servirán peticiones hechas por usuarios registrados en el sistema.

Acto seguido, se comprueba que el servidor FTP está funcionando correctamente mediante esta orden:

```
$ ftp localhost
```

Luego se edita el archivo de configuración **/etc/vsftpd.conf** y se comprueba que están activadas las directivas que determinan el modo de acceso de los usuarios anónimos al servidor FTP con los valores indicados.

Para activar usuarios registrados:

```
local_enable=YES
```

Para desactivar usuarios anónimos:

```
anonymous_enable=NO
```

Los usuarios registrados pueden escribir siempre que los permisos establecidos lo permitan.

```
local_umask=022
```

```
write_enable=YES
```

Si se quiere que los usuarios locales estén en sus propios directorios home cuando se conecten vía FTP, habrá que incluir estas directivas:

```
chroot_local_user=YES
```

```
chroot_list_enable=YES
```

```
chroot_list_file=/etc/vsftpd.chroot_list
```

La primera activa la opción chroot; la segunda, la posibilidad de crear un archivo con los usuarios que no se desea incluir en el entorno chroot; y la última indica el archivo que contiene dicha lista.

A estas directivas habrá que añadir las generales de servidor, así como las utilizadas para la generación de logs y visualización de mensajes.

Para terminar, se eliminarán los comentarios de las directivas correspondientes en el archivo de configuración.