Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Servidor ftp seguro con vsftpd (53306 lectures)

Per **Marie Henri Beyle**, ***mhbeyle*** (http://www.liberaliatempus.com)

Creado el 18/07/2006 23:18 modificado el 18/07/2006 23:18

En este artículo aprenderemos a instalar y configurar un servidor de ftp que viene de serie con numerosas distriuciones: vsftpd (Very Secure FTP Daemon). Como medida de seguridad adicional, aprenderemos a crear usuarios con acceso al servidor que no pertenezcan al sistema. Finalmente, "enjaularemos" a esos usuarios y sólo les permitiremos el acceso a detrminados directorios.

Instalación del servidor vsftpd

Descargamos en instalamos la última versión de vsftpd, bien mediante rpm:

```
# rpm -Uvh  vsftpd-2.0.4-1.2.i386.rpm
```

Bien mediante yum:

```
# yum install vsftpd
```

Ambas opciones dejarán configurado con las funciones básicas un servidor de ftp en nuestro sistema. Para asegurar el inicio del servidor con la carga del sistema, nos serviremos de `chkconfig` en Fedora Core:

```
# chkconfig -add vsftpd
# /etc/init.d/vsftpd restart
```

Por defecto, el servidor ftp "escucha" en el puerto `21`, así que la siguiente orden nos confirmará la ejecución correcta como demonio en el servidor:

```
# netstat -an|grep LISTEN|grep 21
tcp    0 0 0.0.0.0:21    0.0.0.0:*     LISTEN
```

Configuración de las bases de datos

La configuración de los usuarios que van a hacer uso del servidor de ftp ha de estar almacenada en una base de datos. Las preferencias del autor se decantan por dos: Berkeley Database o MySQL. El manual se ocupará de una configuración con Berkeley Database, aunque se darán las indicaciones básicas para una configuración con MySQL (se requerirán ciertos conocimientos de MySQL para crear las bases de datos con los usuarios y sus contraseñas que no serán explicados aquí, por escapar estos al tema principal de este manual).
Lo primero a tener en cuenta será la instalación, si no lo tenemos ya, del soporte para las bases de datos que usemos como almacenamiento de los usuarios. En el caso de usar Berkeley DB instalaremos el soporte que nos ofrece el paquete db4-4.3:

```
# yum install db4 db4-utils
```

En caso de usar MySQL, instalaremos el paquete pam_mysql y todo lo necesario para tener corriendo sin problemas nuestro servidor de MySQL:

```
# yum install pam_mysql
```

Una vez instalado el soporte para las bases de datos, crearemos las tablas contenedoras de los usuarios que usarán el servidor de ftp. Para crear la tabla bajo Berkeley DB, crearemos en primer lugar un archivo de texto plano donde introduciremos, para cada usuario, un par de líneas que contendrán, en este orden, el nombre del usuario y la contraseña. Por ejemplo, un archivo con dos usuarios quedaría como sigue:

```
user_001
passwd001
user_002
passwd002
```

Seguidamente, transformaremos el archivo al formato de Berkeley DB y bloquearemos cualquier acceso al fichero que no sea el del usuario `root` (obviamente, el fichero de texto con las claves será borrado de forma inmediata o guardado en lugar muy seguro):

```
# db_load -T -t hash -f users_db /etc/vsftpd/users.db
# chmod 600 users.db
```

Si vamos a trabajar con MySQL, crearemos la tabla y los pares Usuario/Contraseña correspondientes, recomendándose la introducción de las contraseñas con `encrypt()`.

Configuración de PAM

vsftpd utilizará PAM como pasarela de autenticación hacia la base de datos. Nuestra misión será la creación de un archivo de configuración que le indique a PAM cómo está estructurada esa base de datos y cuál es el mecanismo de acceso a la misma. El archivo de configuración de PAM para *vsftpd* ha de situarse en la ruta `/etc/pam-d/vsftpd` y contendrá las líneas siguientes en el caso de una base de datos Berkeley DB:

```
#%PAM-1.0
auth required /lib/security/pam_userdb.so db=/etc/vsftpd/users
account required /lib/security/pam_userdb.so db=/etc/vsftpd/users
```

Nota: La versión de la librería `pam_userdb.so` utilizada al tiempo de escribir este manual añade la extensión `.db` al archivo de Berkeley DB especificado de forma automática. Es por esto que la ruta que apunta a dicho archivo dentro de `/etc/pam.d/vsftpd` deberá ir sin la extensión `.db`. Esto puede cambiar en versiones futuras de PAM, por lo que, si tenemos algún problema al autenticarnos contra el servidor de ftp, miraremos que en los *logs* del sistema (`/var/log/messages`) no se encuentren errores similares a este: `user_lookup: could not open database `/etc/vsftpd/users.db'` , que se genera a causa del problema descrito.

En el caso de una autenticación con base de datos en MySQL, rellenaremos el fichero con las líneas siguientes:

```
#%PAM-1.0
#user=aduser (Administrador de MySQL)
#passwd=adpass (Contraseña Administrador)
#host=localhost (host MySQL)
#db=db_vsftpd (DB de usuarios de vsftpd)
#table=users (Tabla de usuarios)
#usercolumn=user (Campo con nombre de usuarios)
#passwdcolumn=password (Campo con contraseñas)
#crypt=1 (Mecanismo de encriptación:
#     0 - Texto plano
#     1 - crypt()/encrypt()
#     2 - password() )
auth required /lib/security/pam_mysql.so user=aduser passwd=adpass
host=localhost db=db_vsftpd table=users usercolumn=user passwdcolumn=password
crypt=1
```

```
account required /lib/security/pam_mysql.so user=aduser passwd=adpass
host=localhost db=db_vsftpd table=users usercolumn=user passwdcolumn=password
crypt=1
session required /lib/security/pam_mysql.so user=aduser passwd=adpass
host=localhost db=db_vsftpd table=users usercolumn=user passwdcolumn=password
crypt=1
```

Configuración de vsftpd

El fichero de configuración de vsftpd lo podemos encontrar, en un sistema con Fedora Core, en la ruta `/etc/vsftpd/vsftpd.conf`. No estaría de más echar un primer vistazo a dicho fichero, así como leerse las distintas opciones de configuración ofrecidas mediante la orden `man vsftpd.conf`.

Una vez creadas las bases de datos y los usuarios del servidor ftp, configuraremos vsftpd para bloquear a los usuarios del sistema y permitir el uso de los usuarios virtuales que hemos añadido a nuestra base de datos. Para empezar, haremos algunas modificaciones al fichero `/etc/vsftpd/vsftpd.conf` para adaptarlo a unas necesidades que, a priori, dejarían un fichero como este:

```
#Configuración global de vsftpd
anonymous_enable=NO
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
listen=YES
listen_port=21
local_enable=YES
max_clients=60
max_per_ip=20
pam_service_name=vsftpd
guest_enable=YES
guest_username=virtual
virtual_use_local_privs=YES
user_config_dir=/etc/vsftpd/users
chroot_local_user=YES
local_umask=022
xferlog_enable=YES
xferlog_file=/var/log/vsftpd.log
idle_session_timeout=180
data_connection_timeout=120
ftpd_banner=Welcome to ftp Server
```

Algunas de las opciones listadas tal vez no sean requeridas y puede que tambien necesitemos añadir algunas. Es por esto que vamos a tratar de repasar las distintas opciones a nuestra disposición:

- `anonymous_enable, anon_upload_enable, anon_mkdir_write_enable, anon_other_write_enable`. Estas opciones impiden el acceso de cualquier tipo a usuarios anónimos y del sistema al servidor.
- `listen, listen_port`. Mediante estos parámetros indicamos a *vsftpd* que arranque en modo directo (standalone) y "escuche" en el puerto indicado.
- `local_enable`. Con esta opción permitiremos que los usuarios locales puedan hacer *login* en el servidor. Esto nos servirá para tener un usuario virtual que pueda autenticarse.
- `max_clients, max_per_ip`. Estas opciones nos servirán para establecer el número máximo de clientes, totales y por dirección *IP*.
- `pam_service_name`. Se iguala al nombre con el que hemos guardado nuestro fichero de configuración de PAM dentro de `/etc/pam.d`.
- `guest_enable`. Igualado a `YES`, permite el login de usuarios virtuales.
- `guest_username`. Si se incluye, este parámetro ha de igualarse a un nombre de usuario real hacia el cual se mapearán todos los usuarios virtuales creados. Al crear el usuario, tendremos que igualar su directorio

personal (home) al directorio por defecto que queramos usar como contenedor de archivos. Por ejemplo, para crear un usuario llamado virtual con un directorio en `/var/ftp/pub`, teclearíamos en la consola lo siguiente (El directorio `/var/ftp/pub` ya está creado en algunas distribuciones, así que tendremos que cambiarlo de propietario con el comando `chown`):

```
# useradd -d /var/ftp/pub virtual
```

- `virtual_use_local_privs`. Igualar este parámetro a `YES` supone indicar que los usuarios virtuales tendrán los mismos privilegios que los usuarios locales.
- `user_config_dir`. Igualaremos este parámetro al directorio que contendrá los permisos de cada usuario en un fichero por separado. El formato de cada fichero será el de un fichero de texto plano que contendrá, de todos los parámetros de vsftpd a nuestra disposición, sólo aquellos que queramos que sean aplicados al usuario en concreto. Por ejemplo, dado el fichero `/etc/vsftpd/users/user_001` correspondiente a la configuración de `user_001`, escribiremos las líneas siguientes, donde extendemos los permisos básicos, permitimos la escritura y la subida de archivos y establecemos la raíz a partir de la cuál tendrá acceso dicho usuario:

```
dirlist_enable=YES
download_enable=YES
local_root=/var/ftp/pub/user_001
write_enable=YES
anon_upload_enable=YES
virtual_use_local_privs=YES
```

- `chroot_local_user`. Esta opción se iguala a `YES` para "enjaular" a los usuarios locales en sus respectivos directorios. El usuario "enjaulado" no podrá acceder a nada que esté por encima de su directorio principal. En nuestro ejemplo, el directorio personal del usuario virtual es `/var/ftp/pub` por lo que colgaremos de esa ruta todos los directorios de usuarios virtuales que queramos, ya que no tendrán acceso a ninguna otra parte del disco, ni tan siquiera mediante el uso de enlaces simbólicos.
- `local_umask`. Con esta opción establecemos el valor de umask de los ficheros que se creen mediante el servidor de ftp. Si no utilizamos el parámetro, su valor por defecto será `077`.
- `xferlog_enable, xferlog_file`. Estas opciones activan el log del servidor y lo establecen a un archivo determinado.
- `idle_session_timeout, data_connection_timeout`. Con estas opciones establecemos los tiempos de conexión sin actividad y con ella, respectivamente. Los valores por defecto si no se especifica nada, son de `300` en ambos casos.
- `ftpd_banner`. Mediante esta opción estableceremos un saludo del servidor cuando se produzca una conexión al mismo.

Probando el servidor

Llegados a este punto, tan sólo nos resta conectarnos al servidor y comprobar que nuestra configuración funciona:

```
# ftp localhost
Connected to anna.serverfedora.es.grendell.com.
220 Welcome to ftp anna Server
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (localhost:root): user_001
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Enlace original del artículo: Servidor ftp seguro con vsftpd[1]

Lista de enlaces de este artículo:

1. http://www.liberaliatempus.com/articulos/linux/servidor-ftp-seguro-con-vsftpd.ht

---

E-mail del autor: mhbeyle _ARROBA_ yahoo.es