Parte I: Configuración del servidor vsftpd en Linux-CentOS 6.

El demonio **vftpd** (Very Secure FTP daemon o demonio FTP muy seguro) es un servidor FTP muy utilizado, incluido en diversas distribuciones como Red Hat, Debian o Open Suse, elegido por muchos sitios FTP que necesitan dar cobertura a miles de descargas simultáneamente y al mismo tiempo proteger al servidor de posibles ataques.

La instalación del servicio se basa en el paquete rpm: **vsftpd**. El archivo de configuración del servidor que tendremos que adaptar es: **/etc/vsftpd/vsftpd.conf** .

Sabemos que el acceso al servidor FTP se basa en un proceso de inicio de sesión que utiliza nombres de usuario registrados en el servidor, una vez conectados al servidor FTP los usuarios tendrán los permisos Unix que se hayan establecido sobre los directorios y archivos a los que pueden acceder.

Tipos de usuarios::

a) usuarios con cuentas "reales**"** en el servidor (están **registrados** en **/etc/passwd** y tienen permiso para iniciar sesión (**/bin/bash** como intérprete) y un directorio casa **)** estos usuarios accederán al servidor con su nombre de usuario y contraseña (la de **/etc/shadow**) y en principio, tienen acceso a toda la estructura de archivos raíz (/) del servidor igual que si hubieran iniciado sesión local en el servidor, al registrarse en el servidor FTP **se conectan a su directorio casa**.
Se puede configurar que los usuarios no se muevan por toda la estructura restringiéndoles el acceso sólo a su directorio "**home"** con esta opción: **chroot_local_user= YES**.

b) usuarios **anónimos** sin una cuenta en el archivo **/etc/passwd**, estos usuarios pueden acceder al servidor (si así se configura en el servidor FTP: **anon_upload_enable= YES)** utilizando la cuenta de usuario anónimo registrada en /etc/passwd, sin pemiso para hacer login (**/sbin/nologin);** esta cuenta es la cuenta ftp (**usuario ftp** y **grupo ftp**)
ll /etc/passwd| grep ftp esta cuenta tienen las siguientes características:
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
Los usuarios anónimos se registran con el nombre de **anonymous** sin contraseña o escribiendo cualquier nombre de cuenta de correo válida como contraseña. Al acceder al servidor se conectan al directorio **/var/ftp (este directorio es su directorio raíz /, chroot**) de donde no se pueden mover, podrán acceder a la estructura de directorio que "cuelgue" de **/var/ftp** con los permisos establecidos en los subdirectorios y archivos que contenga. El directorio /var/ftp/ contiene los archivos servidos por vsftpd. También contiene el directorio **/var/ftp/pub/** para los usuarios anónimos. Ambos directorios están disponibles para la lectura de todos, pero sólo root puede escribir en él.

c) usuarios **FTP**, con una cuenta en **/etc/passwd** pero sólo con derecho a hacer FTP, es decir, autorizados sólo a acceder a una parte del sistema de archivos del servidor (por ejemplo su directorio de conexión puede ser: **/var/ftp/nombre-usuario** o **/var/www/html**/**nombre-usu**) sin derecho a login (**/sbin/nologin)** en esos directorios podrán dejar o descargar archivos, páginas web etc, sólo se podrá mover de ese directorio hacia abajo en la estructura de archivos. **vsftpd** reasigna /var/ftp/ al nuevo directorio raíz, conocido como "/**".**

Instalación del paquete rpm vsftpd

Para que el servidor **vsftpd** funcione debemos comprobar que tenemos instalados en el equipo los paquetes rpm correspondientes: **rpm –qa |grep vsftpd** e instalarlos si es preciso: **yum –y install vsftpd**.

Preparar el servicio para que se inicie al arrancar Linux

#chkconfig –level 35 vsftpd on

O desde la herramienta gráfica: **Sistema/Administración/Servicios**

Arranque, parada y reanudación del servicio

#service vsftpd start (stop ó **restart)** o:
#/etc/init.d/vsftpd start (stop ó **restart**)

Cortafuegos

Si el servidor FTP se ejecuta detrás de un cortafuegos, habrá que abrir los puertos FTP (**21/20**) en los que escucha.

Opciones de configuración del archivo: /etc/vsftp/vsftpd.conf

Se debe colocar el símbolo de almohadilla (#) antes de una línea para convertirla en comentario que será ignorada por el servicio.

Cada directiva está en su propia línea dentro del archivo y sigue el formato siguiente:

directiva=valor

Las opciones se habilitan o no, indicando el valor YES o NO, respectivamente. Algunas de las opciones de configuración del servidor son las siguientes:

anonymous_enable=YES => Habilita el que todos los usuarios anónimos pueden acceder al servidor. Se aceptan los nombres de usuario **anonymous** y **ftp**. El valor por defecto es YES

local_enable=YES => Todos los usuarios locales con cuentas reales en el servidor pueden acceder al servidor.

write_enable=YES => Permite a los usuarios con cuentas locales grabar ficheros y directorios en el servidor.

local_umask=022 => Establece los permisos por defecto para los archivos usuarios, si estos pueden grabar.

anon_upload_enable=YES => Permite a los **anónimos** grabar archivos en el servidor. Los ficheros se crean por defecto con los permisos (**600**). Propietario el usuario anonimo (ftp) y grupo (ftp).

anon_mkdir_write_enable=YES => Permite a los usuarios anónimos, crear directorios en el servidor.

anon_umask=máscara => Donde máscara son los permisos con los que los usuarios anónimos van a crear los archivos y directorios.

dirmessage_enable=YES => Se mostrará el mensaje almacenado en el archivo que se especifica en la directiva: **message_file** y por defecto es **.message**, cada vez que un usuario entra en un directorio que tenga un archivo de mensaje.

xferlog_enable=YES => Las conexiones e incidencias se registran en el archivo especificado en la directiva: **vsftpd_log_file=/var/log/vsftpd.log.**. hay que resaltar que si **syslog_enable** está en **YES**, se utiliza el registro del sistema (**/var/log**/messages) en lugar del archivo especificado en esta directiva. El valor por defecto es /var/log/vsftpd.log.

ftpd_banner= Bienvenido al servidor … **=>** Se mostrará el mensaje cuando se conecta el cliente al servidor.

accept_timeout = 60 y **connect_timeout = 60** => cuanto tiempo tiene el cliente para establecer una conexión, antes de que caduque (60 segundos)

idle_session_timeout=600 => se corta la conexión si el cliente lleva 600 segundos (10 minutos) inactivo

local_max_rate=10024 => indica la tasa de transferencia (en bytes) para los
usuarios con cuentas en el servidor, un valor **0** no pone restricciones.

anon_max_rate=10024 => lo mismo pero para los anónimos.

connetc_from_port_20= YES => habilita el puerto 20 para la transferencia de datos.

ls_recurse_enable=YES => activa la opción –R del comando **ls** para que los usuarios puedan listar el contenido de los directorios y de todos los subdirectorios, de forma recursiva.

pasv_enable=YES => habilita el método pasivo

ssl_enable=YES => Permite la utilización de FTP mediante SSL. Requier que vsftpd se haya instalado con soporte OpenSSH.

rsa_cert_file=/etc/ssl/certificado/cert_vsftpd.pem => Indica la ruta al fichero vsftpd.pem que contendrá el certificado RSA para la utilización de conexiones SSL.

rsa_private_keyfile= =>indica la ruta al fichero que contendrá la clave privada RSA para conexiones SSL.

force_local_data_ssl=YES force_local_logins_ssl=YES=> Obliga a la utilización de SSL en todas las operaciones.

Cada vez que se realicen modificaciones en el archivo de configuración **vsftpd.conf** hay que parar y arrancar el servicio, con la opción **restart** (stop/start):
#**service vsftpd restart**

Archivos y directivas del servidor que afectan al control y acceso de usuarios:

- El usuario **root** y otros usuarios administrativos almacenados en el archivo **/etc/vsftpd/ftpusers** no pueden conectarse al servidor, por razones de seguridad. Si queremos negar la conexión a usuarios concretos podemos añadirlos a ese archivo.
- El archivo /**etc/vsftpd.user_list** se puede configurar para negar o permitir el acceso a los usuarios listados, dependiendo de si la directiva: **userlist_deny** está configurada a YES (por defecto) o a NO en /etc/vsftpd/vsftpd.conf.. La directiva: **userlist_deny=YES** cuando se combina con la directiva **userlist_enable =YES** les niega el acceso a los usuarios listados en el archivo especificado por la directiva: **userlist_file=/etc/vsftpd. user_list** antes de que introduzcan el password. (si userlist_deny=NO entonces se deniega a todos excepto a los del archivo que se indique en userlist_file)
- **Modo "enjaulado"**: Si activamos la opción **chroot_local_user=YES** los usuarios trabajarán de este modo al conectarse en el servidor, es decir, sólo se podrán mover de su directorio de conexión (**directorio raíz** o / para ellos) hacia abajo. Si queremos que esta característica no se aplique a algunos usuarios, tendremos que crear el archivo:**/etc/vsftp/vsftpd.chroot_list** y añadir la lista de usuarios. Si se combina con la directiva: **chroot_list_enable=YES** entonces a los usuarios que se especifiquen en el archivo indicado en la directiva: **chroot_list_file= /etc/vsftpd/vsftpd.chroot_list** no les afecta el "modo enjaulado".