INSTALACIÓN Y CONFIGURACIÓN

SERVIDOR VSFTPD
UBUNTU SERVER 20.04

INSTALACIÓN Y CONFIGURACIÓN SERVIDOR VSFTPD

vsFTPd (very secure FTP daemon) es uno de los servidores FTP más potentes y completos disponibles para la mayoría de distribuciones de Linux. Este servidor FTP es el favorito de muchos administradores de sistemas por la configurabilidad que es capaz de proporcionarnos, y por la facilidad de configuraciones avanzadas en el propio servidor FTP.

Para su instalación, en primer lugar debemos obtener las actualizaciones de nuestros paquetes antes de continuar con la instalación del daemon vsftpd.

Cuando termines instala el Daemon vsftpd usando el siguiente comando:

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

INSTALACIÓN Y CONFIGURACIÓN SERVIDOR VSFTPD

Una vez completada la instalación, haz una copia de seguridad del archivo original de configuración en tu carpeta personal.

Este archivo es todo un manual de configuración del servicio, es decir, en cada sección tenemos una pequeña explicación y ejemplo de funcionamiento, parámetro por parámetro. Usadlo (google translator).

A continuación, editamos su fichero de configuración para adaptarlo a nuestras necesidades:

```
sudo vim /etc/vsftpd.conf
```

El fichero de configuración de dicho servidor se encuentra en la ubicación /etc/vsftpd.conf y su configuración por defecto será de sólo lectura, o sea, los usuarios podrán descargar pero no subir ficheros.

Tampoco podremos conectarnos con el usuario *anonymous*. Y por último los usuarios no están *enjaulados* por defecto, o lo que es lo mismo, cualquier usuario que inicie sesión se podrá mover por todos los directorios (esto parece un poco arriesgado en cuanto a lo que seguridad se refiere).

OPCIONES DE CONFIGURACIÓN VSFTPD

Vamos a revisar algunas de las opciones configurables. Las directivas que modifican el comportamiento de vsftpd con respecto a directorios son:

- **download_enable**: cuando está activada se permiten la descarga de archivos.
- **chown_uploads**: si está activada, todos los archivos cargados por los usuarios anónimos pertenecen al usuario especificado en la directriz *chown_username*.
- **chown_username**: especifica la propiedad de los archivos cargados anónimamente si está activada la directriz *chown_uploads*.
- **write_enable**: cuando está activada se permite que los usuarios locales suban o carguen archivos al servidor FTP.
- **dirlist_enable**: al estar activada, los usuarios pueden listar el contenido de los directorios.

OPCIONES DE CONFIGURACIÓN VSFTPD

Las directivas que controlan el comportamiento de los inicios de sesión y los mecanismos de control de acceso son:

- **anonymous_enable**: al estar activada se permite que se puedan conectar los usuarios anónimos. Se permiten los nombres de usuario *anonymous* y ftp.

- **ftpd_banner**: si está activada se muestra la cadena de caracteres especificada en esta directriz cuando se establece una conexión con el servidor.

- **local_enable**: al estar activada los usuarios locales pueden conectarse al sistema.

OPCIONES DE CONFIGURACIÓN VSFTPD

Las directivas que controlan el acceso de usuarios anónimos al servidor son: (para utilizar estas opciones se debe haber puesto la directriz **anonymous_enable** a *yes*).

anon_mkdir_write_enable: Cuando se activa en combinación con la directriz “write_enable”, los usuarios anónimos pueden crear nuevos directorios dentro de un directorio que tiene permisos de escritura.

anon_root: Especifica el directorio al que los usuarios anónimos van a tener acceso. Esta directriz no tiene un valor predeterminado.

anon_upload_enable: Cuando se usa con la directriz “write_enable”, los usuarios anónimos pueden subir archivos al directorio en el que tengan permisos de escritura.

OPCIONES DE CONFIGURACIÓN VSFTPD

Las directivas que controlan el acceso de los usuarios locales al servidor son: (para utilizar estas opciones se debe haber puesto la directriz **local_enable** a *yes*).

chroot_local_user: esta directiva enjaula a los usuarios locales dentro de su propio directorio personal, dichos usuarios solo tendrán acceso a su propio directorio.

chroot_list_enable: cuando está opción esta activada, se enjaulan solo a los usuarios locales listados en el archivo especificado en la directriz **chroot_list_file**.

chroot_list_file: especifica el archivo que contiene una lista de los usuarios locales a los que se quiere enjaular (una línea con el nombre de usuario por cada usuario a enjaular).

local_root: especifica el directorio al cual tendrán acceso los usuarios del servicio ***vsftpd***, siempre y cuando no hayan sido enjaulados previamente.

local_umask: especifica el valor de umask para la creación de archivos subidos al servidor FTP.

USUARIOS PERMITIDOS EN VSFTPD

anonymous_enable=YES/NO
local_enable=YES/NO

La primera indica que cualquier usuario se puede conectar o no al servidor indicando usuario *anonymous* o ftp, y como contraseña una cuenta de correo (o nada). Por defecto el usuario anónimo como ya hemos dicho antes viene deshabilitado. La segunda línea indica que los usuarios locales, es decir con cuenta local, pueden conectarse al servidor (YES).

Vamos a ver como proceder para crear un usuario para el servicio FTP que no pueda loguearse en el sistema (¿qué sentido tiene esto?):

- Para que un usuario tenga acceso al servidor FTP debe ser dado de alta ejecutando un par de líneas similares a las siguientes.

```
sudo useradd -s /usr/sbin/nologin -m alex
sudo passwd alex
```

INSTALACIÓN Y CONFIGURACIÓN SERVIDOR VSFTPD

Como podemos ver, estamos creando un usuario llamado *alex*, el cual no podrá acceder a la línea de órdenes porque le asignamos /usr/sbin/nologin como Shell (consultad el archivo ***/etc/passw*** y ***/etc/shells***)

La opción -m de la primera línea indica al sistema que debe crearse la carpeta personal del usuario que por defecto se ubica en /home y lleva el mismo nombre del usuario. Finalmente la segunda línea permite asignar una contraseña al nuevo usuario.

Hay otras muchas formas distintas de crear usuarios y permisos que podemos asignarles:

- **usermod –d /carpeta/directorio usuario** → asigna el directorio como carpeta personal al usuario.
- **adduser usuario grupo** → asignar un grupo de usuarios a un usuario. O editar el archivo ***/etc/group***.
- **usermod –s /bin/bash usuario** → asigna el shell al usuario

PERMITIR LA SUBIDA DE ARCHIVOS

Por defecto el servidor permite solo la lectura o descarga de archivos pero no la subida.

Con la siguiente línea permitimos la subida a los usuarios anónimos, aunque como ya sabemos esta es una mala política de seguridad para un servidor FTP: **anon_upload_enable=YES**

Si lo que queremos es permitir que los usuarios locales suban o carguen archivos al servidor FTP habrá que habilitar la siguiente directiva: **write_enable=YES**

Cuando habilitamos la subida de ficheros entra en juego otra directiva, **local_umask**. Establece los permisos por defecto para los nuevos archivos y directorios recién creados o subidos al servidor.

Básicamente funciona restando a 777 los permisos que queramos tener, por ejemplo, si queremos que los permisos sean 755, entonces, 777-755=022 (para los propietarios de los archivos, todos los permisos y para el resto, lectura y ejecución). La opción más usada en los servidores ftp es 022, **local_umask=022**

ENJAULAMIENTO DE LOS USUARIOS

Como dijimos en un principio, los usuarios no están enjaulados por defecto, o lo que es lo mismo, cualquier usuario que inicie sesión se podrá mover por todos los directorios (esto parece un poco arriesgado en cuanto a lo que seguridad se refiere).

Para *enjaular* a los usuarios en sus carpetas personales vamos a especificar **chroot_local_user=YES** en el archivo de configuración de ***vsftpd***.

```
# You may restrict local users to their home directories.  See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
#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().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
```

ENJAULAMIENTO DE LOS USUARIOS

La siguiente directriz varía en función del valor de **chroot_local_user**. Si **chroot_local_user=NO** la siguiente directiva especifica que se utilizará una lista con los usuarios locales a los cuales se les enjaulará.

chroot_list_enable=YES

La siguiente directriz (**chroot_list_file**) especifica la ruta donde se encuentra el archivo con la lista de usuarios enjaulados o no enjaulados, según se encuentre la directriz **chroot_local_user**:

- Si **chroot_local_user=NO**, indica la lista de usuarios locales enjaulados, es decir, hay que especificar que usuarios locales queremos enjaular.

- Si **chroot_local_user=YES**, indica la lista de usuarios locales no enjaulados, es decir, todos los usuarios locales estarían enjaulados excepto los de la lista.

chroot_list_file=/etc/vsftpd.chroot_list

ENJAULAMIENTO DE LOS USUARIOS

Una vez establecidas dichas directivas, solo queda añadir las cuentas de usuario al fichero de usuarios **/etc/vsftpd.chroot_list**, el formato que debe tener es de una línea con el nombre de la cuenta de usuario por cada usuario.

Algunos enlaces con más información:

http://vsftpd.beasts.org/

https://sio2sio2.github.io/doc-linux/07.serre/01.ftp/02.vsftpd.html

https://blog.infranetworking.com/servidor-ftp-linux/

https://www.especialistashosting.com/blog/2012/03/crear-carpetas-y-usuarios-ftp/

https://www.redeszone.net/tutoriales/servidores/vsftpd-configuracion-servidor-ftp/

https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-ftp-vsftpd-conf.html

MÁS PARÁMETROS PARA USUARIOS ANÓNIMOS

anon_mkdir_write_enable=YES # permite a los usuarios anónimos a crear carpetas.

anon_other_write_enable=YES #Permite al usuario ftp/anonymous borrar.

anon_root=/ftp/anonimo # 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.

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

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

MÁS PARÁMETROS PARA USUARIOS ANÓNIMOS

Podemos mediante la opción **anon_root** darle al usuario *anonymous* (ftp) un directorio donde trabajar, por ejemplo, ***/ftp/anonimo***.

Debemos crear el directorio mediante el comando ***mkdir***, por ejemplo:

```
sudo mkdir /ftp
sudo mkdir /ftp/anonimo
sudo mkdir /ftp/anonimo/subidas
```

Y darle los permisos que estimemos oportunos mediante el comando ***chmod***. Los permisos que le demos a los directorios deben coincidir con la configuración de permisos del archivo de configuración ***vsftpd.conf***.

Además, el directorio donde iniciar el usuario ***ftp/anonymous*** no puede tener todos los permisos por motivos de seguridad, sino al iniciar sesión en el servidor ftp es posible que de el siguiente error (500 OOPS: vsftpd : refusing to run with writeable root inside chroot()).

MENSAJES

Al conectarse un usuario al servicio FTP y hacer un cambio de directorio dentro del directorio raíz de descargas se puede visualizar un mensaje cuyo texto se almacena en el archivo .mensaje. Para ello debemos:

Crear el archivo .mensaje e incluir en él el texto que se quiera.

Incluir las directivas siguientes en el archivo de configuración:

dirmessage_enable=YES

message_file=rutadel fichero

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

ftpd_banner= ”Bienvenido a mi servidor FTP”

LIMITACIONES

Podemos limitar la velocidad de transferencia de ficheros, tanto para usuarios locales como anónimos con las directivas:

local_max_rate=7200

anon_max_rate=2048

El número indica bytes/seg. En caso de no indicar nada la velocidad será ilimitada.

Con respecto a las conexiones:

max_clients=3 #Numero máximo clientes conectados.

max_per_ip=2 #Numero máximo de conexiones por IP.

TIEMPOS DE INACTIVIDAD

accept_timeout=60 indica, en segundos, el tiempo para establecer una conexión de un usuario remoto. Por defecto son 60 segundos.

data_connection_timeout=300 indica, en segundos, tiempo máximo que el servidor espera cuando una transferencia no progresa. Por defecto son 300 segundos.

idle_session_timeout=300 indica, en segundos, tiempo máximo concedido a un usuario remoto que no está activo, es decir, no está ejecutando órdenes FTP. Pasado este tiempo se corta la conexión. Por defecto son 300 segundos.

REGISTROS DE ACTIVIDAD

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

xferlog_enable=YES # Activa la generación de registros logs por cada upload/download.

vsftpd_log_file=/var/log/vsftpd.log # Define cual será el archivo log.

log_ftp_protocol=YES # Si esta directiva no se encuentra comentada activa el registro (log) de todas las peticiones/respuestas del servidor.

A continuación debemos reiniciar el servidor para que se tengan en cuenta estos cambios:

```
sudo /etc/init.d/vsftpd restart
```

También es posible añadir cuotas de descarga.

OTRAS CONFIGURACIONES

En caso de estar detrás de un firewall debemos configurarlo, si se trata de UFW con el comando:

```
sudo ufw allow ftp
```

Esa regla solo permite conectar en modo activo, debemos abrir un rango de puertos para usar el modo pasivo que posteriormente configuraremos en ***vsftpd***. Por ejemplo, abriendo puertos del 30.000 al 30.050.

```
sudo ufw allow 30000:30050/tcp
```

Para configurar el modo pasivo debemos añadir las directivas:

pasv_enable=YES

pasv_min_port=30000

pasv_max_port=30050

INSTALACIÓN Y CONFIGURACIÓN SERVIDOR VSFTPD

IES Los Albares

FIN