1 Servidor FTP vsftpd

vsftp ou (Very secure FTP) supostamente é o servidor FTP máis seguro para o mundo Linux/Unix, en canto a seguridade, rendemento e escalabilidade.

Soporta o uso de certificados dixitais SSL, sempre e cando o cliente ftp os soporte (empregar o cliente ftp-ssl en vez de ftp). Unha das peculiaridades que permite, e o uso de gaiolas chroot para os usuarios. Unha gaiola chroot, establece un directorio determinado como directorio raíz. Desde ese directorio, non se poderá acceder a ningún de nivel superior, pero si a todos os descendentes.

1.1 Sumario

- 1 Instalación
- 2 Configuración básica
  - 2.1 Mensaxe de benvida
  - 2.2 Habilitación de escritura
  - 2.3 Permisos dos ficheiros e directorios resultantes
- 3 Gaiolas *chroot*
  - 3.1 Gaiolas *chroot* so para certos usuarios
  - 3.2 Mensaxes de erro asociadas a *chroot*
- 4 Acceso anónimo
- 5 FTP seguro
- 6 Restriccións FTP
  - 6.1 Cotas de disco
- 7 Logs
- 8 Outras referencias

1.2 Instalación

Para instalalo, en Linux, temos que instalar o paquete *vsftpd*

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

1.3 Configuración básica

Os ficheiros que temos que editar para configurar o servidor son */etc/vsftpd.conf* ou */etc/vsftpd/vsftpd.conf*

Unha vez editado o ficheiro de configuración, e feito algún cambio, estes aplícanse reiniciando o servidor:

```
sudo service vsftpd restart
```

Tamén se pode configurar desde o Webmin, pero habería que instalar o módulo correspondente, módulo que non ven na instalación por defecto de Webmin. Podes descargar o módulo vsftpd e instalalo no Webmin no apartado de módulos.

Por defecto, poden acceder ao servidor FTP todos os usuarios do sistema, en modo so lectura.

1.3.1 Mensaxe de benvida

Podemos establecer unha mensaxe de benvida para os usuarios que se conectan ao sistema:

```
ftpd_banner=Bienvenido ao servidor FTP
```

ou especificando un ficheiro de texto, onde se gardará a mensaxe a amosar como benvida (útil no caso de ocupar varias liñas)

```
banner_file=/etc/vsftpd/welcome.banner
```

1.3.2 Habilitación de escritura

Por defecto, a escritura no sistema está deshabilitada. Para habilitala incluímos a seguinte directiva.

```
write_enable=YES
```

Para os usuarios locais, esta directiva habilita tanto a subida de ficheiros, coma a creación de directorios e o renomeado.

1.3.3 Permisos dos ficheiros e directorios resultantes

O *umask* para os usuarios locais está establecido a **077**. Podemos configuralo a outro valor coa directiva

```
local_umask=022
```

Estes permisos sempre se van a restar, do valor que teña a directiva **file_open_mode** que por defecto ten o valor **0666** (sempre elimina os permisos de execución).

1.4 Gaiolas *chroot*

Os usuarios, por defecto, poden acceder a todos os cartafois e directorios nos cales teña permiso de lectura e acceso. Pero podemos limitar esa característica ao seu directorio persoal. Isto é o que se coñece como establecer unha gaiola *chroot*. Configúrase coa directiva

```
chroot_local_user=YES
```

1.4.1 Gaiolas *chroot* so para certos usuarios

Se queremos que so certos usuarios teñan activado *chroot*, establecemos a directiva

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/users.list
```

e no ficheiro */etc/vsftpd/users.list* teremos unha lista dos usuarios afectados por *chroot*

- Se a directiva **chroot_local_user** aparece no ficheiro e ten o valor **YES** a lista conten os **usuarios que non teñen activado chroot**
- Se a directiva **chroot_local_user** non aparece no ficheiro ou ten o valor **NO** a lista conten os **usuarios que teñen activado chroot**

1.4.2 Mensaxes de erro asociadas a *chroot*

Se aparece un erro ao acceder os usuarios locais con esta mensaxe **500 OOPS: vsftpd: refusing to run with writable root inside chroot()** débese a que *vsftpd* non permite que os usuarios poidan escribir na súa carpeta raíz. Unha solución é quitarlle os permisos de escritura a esa carpeta. Isto fará que o usuario non poida facer nada na súa propia carpeta, así que o mellor é crearlle outra dentro con permisos normais para que poida escribir nela.

A outra alternativa para solucionar ese erro é engadir a directiva.

```
allow_writeable_chroot=YES
```

 Esta directiva so estará dispoñible se a versión do servidor é a 3 ou superior.

O usuario anónimo sempre conectará dentro dunha contorna *chroot*. E sempre será necesario que **non teña permiso de escritura no seu HOME**.

Se nos aparece o erro:

```
500 OOPS: priv_sock_get_cmd
```

deberemos engadir a liña

```
seccomp_sandbox=NO
```

Isto é un coñecido bug, que hai en versións 3.0.x con arquitectura amd64.

1.5 Acceso anónimo

Podemos tamén habilitar o acceso a usuarios anónimos, que por defecto ven deshabilitado. Habilitámolo coa directiva

```
anonymous_enable=YES
```

O usuario anónimo, está engaiolado no directorio raíz (HOME) do usuario *ftp* do sistema. Tamén podemos facer que inicie sesión noutro directorio

```
anon_root=/ruta/ao/directorio/onde/iniciara/sesion/o/usuario/anonimo
```

Por defecto, o usuario *anonymous* non pode subir arquivos. Se queremos permitir que os usuarios anónimos poidan subir arquivos ao servidor teremos que ter en conta que:

- O usuario ftp non debe ser propietario do directorio onde se suban os ficheiros.
- O usuario ftp non debe ser membro do grupo propietario do directorio onde se suban os ficheiros.
- O directorio anónimo debe ter os permisos de escritura correspondentes para OUTROS.

Para permitir a escritura ao usuario anónimo, tendo en conta o anterior, temos que habilitar a directiva

```
anon_upload_enable=YES
```

Se a maiores, queremos permitir que poida crear directorios, empregamos a directiva

```
anon_mkdir_write_enable=YES
```

O usuario propietario dos ficheiros subidos será o usuario *ftp* . Tamén podemos facer que o usuario propietario dese arquivo sexa calquera outro dos presentes no sistema. Iso consíguese coa directiva:

```
chown_uploads=YES
chown_username=whoever
```

Recoméndase que o usuario propietario non se cambie a *root*

1.6 FTP seguro

Tradicionalmente, o servizo FTP sempre foi inseguro. Cando un usuario se conecta, o seu nome de usuario e contrasinal, son transmitidos sen encriptar, podendo pasar, que alguen intercepte a comunicación e se faga coas credenciais do usuario. Afortunadamante, pódese empregar facendo que o servidor FTP empregue autenticación de OpenSSL, facendo que o nome de usuario, o seu contrasinal e tamén os datos transferidos vaian encriptados.

Para conseguir isto, o primeiro paso é crear o certificado SSL,

```
 sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/certs/vsftpd.pem
```

A continuación editamos o ficheiro de configuración de vsftp e introducimos as seguintes directivas (Se algunha delas está configurada, eliminámola):

```
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=NO
force_local_logins_ssl=NO
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
rsa_cert_file=/etc/ssl/certs/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
```

Se queremos forzar a que os usuarios locais so se poidan conectar empregando SSL, cambiamos as seguintes directivas.

```
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

Cando se realice a conexión, pode verse o algoritmo de encriptación empregado:

```
220 Welcome to blah FTP service.
 Name (192.168.56.253:bruno): adminlocal
 234 Proceed with negotiation.
 [SSL Cipher DES-CBC3-SHA]
 331 Please specify the password.
 Password:
```

Todo o que se transmita por esta canle, queda encriptado.

1.7 Restriccións FTP

No servidor vsftpd, podemos restrinxir o acceso por parte dos usuarios, coas seguintes directivas

- Para restrinxir o número de clientes conectados de forma simultánea:

```
max_clients=5
```

- Para limitar o número máximo de conexións que se poden realizar desde un mesmo enderezo IP. Hai que ter en conta que algunhas redes acceden a través dun servidor proxy ou porta de ligazón e debido a isto poderían quedar bloqueados innecesariamente algúns accesos:

```
max_per_ip=4
```

- Para limitar o ancho de banda de descarga para os usuarios locais e o usuario anónimo (en bytes por segundo). Por defecto, o valor é 0, o cal significa que non hai límite:

```
local_max_rate=5120
anon_max_rate=4096
```

- Para establecer un tempo de espera para manter establecidas conexións inactivas.

```
idle_session_timeout=600
```

- Para establecer un tempo de espera para manter establecidass conexións de datos inactivas.

```
data_connection_timeout=120
```

- Para activar/desactivar conexións pasivas

```
pasv_enable=YES
```

1.7.1 Cotas de disco

Tamén podemos establecer cotas de disco para os distintos usuarios. Para máis información, acceder ao seguinte enlace

1.8 Logs

Por defecto vsftpd garda un log de todas as cargas/descargas no ficheiro *=/var/log/vsftpd.log*. Se queremos cambiar esa configuración temos estas dúas directivas:

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

1.9 Outras referencias

1. Páxina de manual de vsftpd.conf
2. Opcións de configuración de vsftpd
3. Manual de vsftpd