

# VSFTPD

És el servidor ftp que inclou Red Hat. VSFTP són les sigles de Very Secure FTP Daemon, per tant, aquest servidor de ftp prima la seguretat en les transmissions d'arxius.

## **Instal·lació**

Al igual que altres eines que ja hem vist, podem instal·lar VSFTP utilitzant paquets RPM. Trobarem aquests paquets en els CD's d'instal·lació de Red Hat. També podem instal·lar-lo directament des de l'entorn gràfic utilitzant la utilitat afegir/eliminar aplicacions.

Com ja hem comentat, l'arxiu de configuració es troba a /etc/vsftpd/vsftpd.conf. Amb aquest arxiu regularem el funcionament del servidor de ftp. Veurem l'efecte de les clàusules més importants.

## **L'arxiu de configuració de vsftpd**

L'arxiu de configuració de vsftpd es troba a:

```
/etc/vsftpd/vsftpd.conf
```

Cada vegada que hi moidiquem alguna cosa, caldrà executar l'script per reanarcar:

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

El primer que farem serà assegurar-nos que estem treballant en mode "standalone". És a dir des del servidor ftp contra ell mateix. Si no treballéssim en aquest mode, vsftpd estaria controlat per xinetd.

Editem l'arxiu de configuracions i ens assegurarem que hi sigui la línia

```
listen=YES
```

```
anonymous_enable=NO/YES
```

Activa o desactiva l'accés FTP anònim. Si no tenim clar que volem donar accés a qualsevol al nostre servidor, serà millor establir aquesta opció a "NO".

```
local_enable=NO/YES
```

Aquesta opció activa o desactiva la capacitat de que els usuaris locals puguin accedir al servidor FTP. És a dir, posant YES o NO podem deixar que els usuaris que tinguin compte a la màquina puguin connectar-se al servei FTP o no. Normalment aquesta opció s'establirà a "YES".

```
write_enable=NO/YES  
anon_upload_enable=YES
```

Activa o desactiva la opció per escriure al servidor FTP. Si volem poder pujar informació al servidor, fixarem aquesta opció a "YES".

L'altra clàusula (anon\_upload\_enable) serà la que activarem si volem que l'usuari anònim pugui realitzar càrregues (pujar arxius) al servidor ftp

```
local_umask=022 # O
```

La umask por defecte és 077. Establim una umask personalitzada pels fitxers creats.

```
xferlog_enable=YES
```

Activa el registre (log històric) dels arxius que pugen al servidor i les descàrregues realitzades.

```
ftpd_banner=Benvingut al meu servidor FTP
```

Permet establir un missatge de benvinguda personalitzat als usuaris quan es connectin al servidor.

```
chroot_list_enable=NO/YES  
chroot_list_file=/etc/vsftpd.chroot_list
```

Aquesta directiva ens permet definir una llista d'usuaris (la que es defineix a la segona comanda `chroot_list_file`). Tots els usuaris que es trobin en aquesta llista estaran limitats a poder accedir únicament al seu directori home. Aquesta sentència serà útil per evitar que els usuaris accedeixin al sistema i limitar-los únicament al seu directori. Ens permetrà definir una política de privacitat i de seguretat.

```
userlist_enable=NO/YES  
userlist_deny=NO/YES
```

L'opció "userlist\_enable" indica a vsftpd si consultarà o no els arxius `vsftpd.ftpusers` i `vsftpd.user_list`. Si activem aquesta opció els dos arxius funcionen com una llista d'usuaris que estan autoritzats a connectar-se al servidor FTP. Per contra, si activem l'opció "userlist\_deny=YES", els dos arxius indicats funcionen com una llista d'usuaris que NO estan autoritzats a connectar-se al servidor FTP. Aquesta opció és molt útil per negar completament l'accés FTP a usuaris crítics del sistema com "root", "apache" o "www". Aquesta és una molt útil mesura de seguretat per al servidor FTP.

A més d'aquestes sentències n'hi ha d'altres que ens permetran configurar les velocitats i taxes de transferència per usuaris, el nombre màxim d'usuaris i altres configuracions.

## ***Els arxius de configuració vsftpd.ftpusers i vsftpd.user\_list***

Com ja hem comentat aquests dos arxius s'enllacen amb les opcions "userlist\_enable" i "userlist\_deny" a l'arxiu de configuració `/etc/vsftpd/vsftpd.conf`. Quan l'opció "userlist\_enable" es posa a "YES", aquests dos arxius funcionen com una llista d'usuaris que estan autoritzats a connectar-se al servidor FTP. En canvi, quan activem l'opció "userlist\_deny=YES" funcionaran com una llista d'usuaris que NO estan autoritzats a connectar-se al servidor FTP. Quan utilitzem l'opció "userlist\_deny", la natura de la denegació de servei FTP que un usuari rep serà diferent depenent de l'arxiu en el que estigui llistat.

Si un usuari està llistat a l'arxiu `vsftpd.user_list` i l'opció "userlist\_deny" està activada, a aquest usuari ni tant sols se li demanarà contrasenya quan intenti connectar-se al servidor FTP. Se'l rebutjarà d'entrada.

Si l'usuari es troba a l'arxiu `vsftpd.ftpusers` i l'opció "userlist\_deny" està activada, se li demanarà la contrasenya, però no li deixarem iniciar sessió.

## ***L'arxiu de configuració vsftpd.chroot\_list***

Quan utilitzem aquest arxiu juntament amb l'opció "chroot\_list", estableix una llista d'usuaris que seran confinats a treballar únicament al seu directori home, sense poder accedir a cap més directori del sistema. Aquesta serà una bona opció quan treballem en un entorn FTP compartit on requerim privacitat.

No cal perdre de vista que cada vegada que efectuem modificacions als arxius de configuració, caldrà reiniciar vsftpd

## Comentaris de l'instal·lació

Una vegada tot instal·lat, ens pot aparèixer el següent missatge:

```
530 Must perform authentication before identifying USER
```

Si apareix, haurem d'utilitzar ntsysv (eina gràfica per activar/desactivar serveis) i farem:

- deseleccionar gssftp (part de l'autenticació – servidor IMAP)
- seleccionar vsftpd

Després d'això executarem l'script de xinetd (/sbin/service/xinetd reload)

També ens pot aparèixer el missatge:

```
530 Please login with USER and PASS KERBEROS_V4
```

Al client escriurem **passive**, d'aquesta forma desactivarem el mode passiu.

Podrem cridar al servidor, des del client fent:

```
ftp usuari:contrasenya@servidor
```

## FTP anònim

Anem a veure els passos a seguir per permetre l'accés de l'usuari anònim a fitxers del sistema via ftp:

- 1) crear un usuari ftp i un grup d'usuaris ftp:  
\$ groupadd ftp  
\$ useradd -m -r -g ftp ftp (-r fa que tingui un UID petit)
- 2) assegurar-nos que el directori /var/ftp (que serà el directori de treball de l'usuari ftp)tingui directoris pub, bin, lib i etc  
\$ mkdir /var/ftp/pub /var/ftp/bin /var/ftp/lib /var/ftp/etc
- 3) fixar propietaris i permisos necessaris:  
\$ chown root.root bin etc lib  
\$ chown root.ftp pub  
\$ chmod 111 bin etc (--x -x -x)  
\$ chmod 755 lib (rwx r-x r-x)  
\$ chmod 2755 pub (2→ permisos especials: executar agafant UID del propietari)
- 4) ficarem al directori /var/ftp/bin els arxius binaris que volem fer accessibles per qualsevol
- 5) ficarem al directori /var/ftp/lib les llibreries que volem fer accessibles per qualsevol
- 6) comprovar que, entrant a ftp des del client amb usuari anonymous, ens deixa accedir a tot el que penja de /var/ftp, ja que, quan s'entra a ftp amb usuari anonymous, es va directament a /var/ftp. Ens permetrà entrar però veurem que hi ha restriccions

Si no funciona, assegurar:

- que l'usuari ftp, a l'arxiu /etc/passwd tingui com a directori de treball /var/ftp.
- assegurar que /var/ftp tindrà permisos de lectura per a l'usuari ftp
- assegurar que l'usuari ftp tindrà permisos per llegir tot el que penja de /var/ftp
- 

També tenim la possibilitat inversa, és a dir, permetre a l'usuari anònim ficar arxius al sistema via ftp:

- 1) Creem un directori per gravar la informació que l'usuari vulgui copiar al sistema  
\$ mkdir /var/ftp/incoming
- 2) Donem la propietat i els permisos necessaris:  
\$ chown root.ftp incoming  
\$ chmod 730 incoming (fem que ftp pugui escriure però l'usuari anònim no pugui llegir)
- 3) Permetim pujar arxius al sistema  
Ens haurem d'assegurar que a l'arxiu /etc/vsftpd/vsftpd.conf haguem activat:

```
write_enable=YES  
anon_upload_enable=YES
```

- 4) Ens connectem a ftp amb usuari anònim i comprovem que podem gravar arxius a /incoming, però no el podem llegir ni tornar a baixar. Tampoc podem pujar arxius a altres directoris