Activitat Formativa AF.3.1- Instal·lació / configuració d'un servidor FTP/S

Índex

1. Introducció

El servidor FTP per a Linux que tractarem en aquesta pràctica és el **vsftpd** (Very Secure FTP Daemon). Aquest servidor destaca per la seva senzillesa, facilitat d'ús, configuració i, sobretot, per la seguretat. És utilitzat per importants llocs a Internet que han de suportar gran quantitat de connexions anònimes simultànies. Per exemple, és el que s'utilitza per al projecte Debian (ftp.debian.org), pel projecte GNU (ftp.gnu.org) o per l'empresa Red Hat (ftp.redhat.com) Entre d'altres.

2. Instal·lació del servei

Durem a terme la instal·lació del servei mitjançant el gestor de paquets del sistema operatiu

```
$ sudo apt install vsftpd;
```

Després de la instal·lació es crearà automàticament un usuari anomenat ftp i una carpeta local /srv/ftp, que ens servirà per a connectarnos al servidor quan fem ús de la funció **d'usuari anònim** (podem veure les seves característiques al fitxer /etc/passwd).

```
$ cat /etc/passwd
```

```
ftp:x:111:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

Activitat 1

Contesta breument i amb les teues paraules la següent **qüestió**:

- Què significa l'última opció de l'usuari **FTP** que apareix al fitxer **/etc/passwd** /usr/sbin/nologin
- On podem trobar el **fitxer principal** de configuració del servidor **vsftpd**? Pots consultar la documentació oficial ací

Per gestionar el dimoni del **vsftpd** utilitzarem el comandament systemctl o el seu corresponent service

systemctl [start|stop|restart] vsftpd	service vsftp [start|stop|restart]

3. Configuració del servidor

En primer lloc, i abans de fer cap canvi al fitxer de configuració, crearem una còpia de seguretat del fitxer principal **vsftpd.conf**

```
$sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.back
```

Com als serveis configurats a les darreres unitats, les línies d'aquest arxiu segueix el següent patró: `directiva=valor`, on **directiva** és el nom de la propietat que es vol configurar, i **valor** serà el valor que se li assigna en qüestió a aquesta directiva.

És important remarcar que no hi ha espais en blanc ni abans ni després del símbol "=", en cas contrari, no s'assignarà el valor de forma correcta, i la directiva tindrà un valor nul·l.

Entre les opcions, podrem comprovar que algunes d'elles són booleanes, i el camp valor pot contenir YES o NO. Altres seran numèriques i altres seran de tipus cadena de caràcters.

3.1 Directives més importants

3.1.1 Gestió d'usuaris

Els **usuaris per defecte** que poden utilitzar per a connectar-nos al servici ftp **són els anònims i els usuaris locals** (recordem que aquestos últims disposen d'un compte en el sistema). Les següents línies ens serviran per establir si habilitem o no aquests 2 tipus d'usuaris.

```
# Habilita/Deshabilita els usuaris anònims al servidor
anonymous_enable=NO
# Habilita/Deshabilita els usuaris amb compte local a la màquina
local_enable=YES
```

Si visualitzem el fitxer de configuració, per defecte, els usuaris locals tenen habilitat el seu accés, però l'usuari **anònim** apareix desactivat. En **vsftpd** aquest usuari es diu 'anonymous' o 'ftp' i la **contrasenya no és necessària**.

3.1.2 Usuaris anònims

Quan un usuari anònim (**anonymous** o **ftp**) es connecta al servidor, aquest usuari anirà per defecte al directori `/srv/ftp`. Dit usuari s'executa sota l'entorn o ambient d'una **"gàbia" chroot**, el que significa que **aquest directori serà el directori arrel al que es conectarà i que no podrà eixir d'ell.**

Activitat 2

- Quina directiva podríem utilitzar per a canviar el directori per defecte al que es connectarà l'usuari anònim? Mira en la documentació oficial
- Activa l'accés anònim només de lectura a la carpeta per defecte**.** Crea un fitxer **prova.txt** i comprova el correcte funcionament.

Donat que, per defecte, el servidor funciona en mode passiu, limitarem els ports del servidor que pot gastar per a l'establiment de connexions, de forma que ens permeta obrir menys ports al firewall.

```
#Port mínim que pot ser assignat per a la connexió de dades
pasv_min_port=40000
#Port màxim que pot ser assignat  a la connexió de dades
pasv_max_port=50000
```

El següent pas serà **obrir els ports** corresponents ports al **firewall**

```
$ sudo ufw allow 20/tcp
$ sudo ufw allow 21/tcp
$ sudo ufw allow 990/tcp
$ sudo ufw allow 40000:50000/tcp
```

Activitat 3

Indica en quin mode de connexió es fa ús de cada una de les regles del firewall anterior i per a que es gasten (dades o control)

3.1.3 Gestió d'usuaris locals

Si **activem els usuaris locals** i volem que **només alguns** dels **usuaris** del sistema puguen connectar-se els incorporarem al fitxer **/etc/vsftpd.userlist** i usarem la directiva userlist_deny, Aquesta directiva ens permet definir si el usuaris que fiquem al fitxer **/etc/vsftpd.userlist** son usuaris als quals se'ls permet la connexió o, pel contrari, es tracta de usuaris als quals no es permetrà la connexió. A continuació, analitzarem les **2 opcions disponibles:**

La directiva **userlist_deny** permet invertir la lògica de la llista d'usuaris, de forma que si s'estableix a **NO,** sols permetrà la connexió d'aquells usuaris que apareixen al fitxer.

Opció A – Definició d'una llista d'usuaris als quals se'ls permet la connexio via ftp

```
#Estableix que l'arxiu /etc/vsftpd.userlist representa una llista d'inclusió d'usuaris
```

```
que no tindran accés per FTP
userlist_deny=NO
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
```

Opció B - Definició d'una llista d'usuaris als quals no se'ls permet la connexio ftp

```
#Estableix que l'arxiu /etc/vsftpd.userlist representa una llista d'exclusió d'usuaris
userlist_deny=YES
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
```

3.1.3.1 Descàrrega d'arxius i establiment de carpetes i permisos

Els usuaris locals, per defecte, podran descarregar-se arxius del directori /srv/ftp, **segons els permisos que tingui el directori o subdirectoris**, i dels permisos dels arxius que es troben allà.

En moltes ocasions, és molt probable que necessitem engabiar un **usuari local** del sistema dins del seu propi **home** o, a la **carpeta de desplegament** del seu web. Per poder fer-ho, haurem d'activar la següent directiva:

```
#Limita l'accés als usuaris locals a la home de l'usuari amb en el que estem connectant-se
chroot_local_user = YES
```

3.1.3.2 Pujada d'arxius per als usuaris locals

Si **volem permetre que els usuaris locals puguen pujar arxius al servidor FTP i, més concretament, al directori configurat** caldrà habilitar la següent directiva i assegurar-se de que l´usuari té permisos d'escriptura al directori.

```
#Permet l'escriptura en el servidor
```

```
write_enable=YES
```

Solució a l'error 500 OOPS: vsftpd: refusing to run with writable root inside chroot()

Aquest error és dona per com **vsftpd** gestiona la seguretat, no permetent que els usuaris escriguen en la **carpeta arrel** en la qual hem **"engabiat"** l'usuari. Per solucionar-lo, crearem una carpeta **FTP** en cada home de l'usuari en la que no tinguem permisos d'escriptura i ficarem que el directori de connexió arrel per a quan realitzem la connexió FTP per a cada usuari és: /home/{usuari}/ftp.

```
#Establim que puga utilitzar-se el contingut de $USER com a part del directori d'usuari
user_sub_token=$USER

#Establim un nou directori arrel per a l'usuari
local_root=/home/$USER/ftp
```

Però quan un usuari carregue un arxiu al servidor, **¿Quins permisos tindrà el fitxer? La** contestació a aquesta pregunta és bastant fàcil, nosaltres podrem establir mitjançant una directiva els permisos amb els quals quedaran els arxius que pugin els usuaris. Aquesta directiva és:

```
# Estableix la màscara aplicable per als arxius carregats
local_umask = 022
```

Com veiem aquesta directiva fa referència a la màscara (umask), i igual que la comanda **umask** de Linux, això ens indicarà els permisos que tindrà el fitxer de forma inversa. És a dir, si volem establir que els fitxers tinguen permisos 755, li donarem un umask de 022**.** Això ens indicarà que els permisos dels fitxers enviats seran 644 (lectura i escriptura per a l'usuari propietari, i només lectura per al grup propietari i per a la resta d'usuaris). Podríem preguntar-nos per què no és **755**; per això, cal recordar que per defecte els **arxius** es creen creem amb **666** i no **777** com ocorre als directoris. Per tant, amb un umask de 022 els fitxers i directoris quedarien:

Tipus	Permisos per defecte	Màscara (umask)	Permisos obtinguts (PD -

	(PD)		umask)
Fitxer	666	022	**(666-022)** → 644
Directori	**777**	022	**(777-022)** →)755

Activitat 4

Per què creus que volem que al pujar un fitxer **al document root d'un virtual host** els permisos de directori siguin 755 i els de fitxer 644? Com faries perquè els fitxers es pujaren amb un nivell de seguretat major, es a dir amb permisos de directori **751** i de fitxer **640?** (no cal que ho facis)

3.1.3.3 Registre d'activitat (Fitxers de Log)

Mitjançant el registre d'activitat podrem portar un control sobre el qual succeeix al nostre servidor FTP. Aquest registre es troba a l'arxiu /var/log/vsftpd.log i les directives per gestionar-lo són les següents:

```
#Activa/Desactiva el registre d'activitat de les càrregues i descàrregues
xferlog_enable=YES
# Localització del fitxer de logs
xferlog_file=/var/log/vsftpd.log
# Activa/Desactiva el log per al protocol vsftpd
log_ftp_protocol=YES
```

Per visualitzar la informació d'activitat haurem d'accedir al contingut del fitxer indicat, fins i tot **el podem mantenir obert visualitzant les últimes línies del fitxer**, és a dir, l'activitat que s'està registrant en aquest mateix moment. El registre d'activitat ens servirà per realitzar posteriors estudis i estadístiques sobre l'ús del servidor, encontrar errades, etc.

Amb l'execució del següent comandament ens podrem veure l'escriptura del log en temps reial

```
$ tail -f /var/log/vsftpd.log
```

4. Configuració d'una infraestructura de desplegament web per FTP

En aquesta última part, simularem la configuració del hosting de **000webhost** que vam utilitzar a la pràctica anterior. És a dir, **configurarem una infraestructura que ens permetrà donar a un client un compte per a connectar amb un usuari per FTP** que el portarà al **Document Root d'un servidor Apache, on podrà pujar i publicar el seu web**, d'aquesta forma podrem compartir el servidor web amb diferents usuaris tal com vam veure a la pràctica anterior.

Activitat 5

Crea un usuari local del sistema en una màquina **Ubuntu-server** anomenat empresa-client. Seguidament, crea un nou vhost **001-es-empresa-client-web,** on **001** és el contador manual del hosts virtuals de la teva màquina. El **documenRoot** serà /home/empresa-client/www/html. El **nom de domini** que configurarem per a aquest (nou) virtual host serà www.empresa-client.es

- Insta-la i configura un **servidor vsftp** perquè els **usuaris locals** puguin iniciar sessió i pujar arxius al servidor.
- Configura el **chroot** del servidor **ftp** perquè, quan un usuari es connecti al servidor, ho faça directament a la **carpeta anterior a la que hem configurat el document root** /home/empresa-client/www/**.** Seguidament activa la directiva perquè quede **"engabiat"** de forma que quan es connecte per FTP sols puga pujar arxius a aquest directori. Recorda que:
  - Has de llevar-li permissos d'escriptura a l'usuari de connexió en aquesta carpeta, en cas contrari, et donarà l'error esmentat en el *punt 3.1.3.2 (es a dir deixarem permisos de lectura i execució sobre la carpeta*)**.**
  - L'usuari ha de tenir permissos d'escriptura en el document root /home/empresa-client/www/html per a poder pujar el web per ftp.
- Fes que quan aquest usuari puje fitxers al document root, tinguin permisos 755. D'aquesta forma l'usuari www-data amb el que Apache serveix les peticions podrà accedir sense cap problema.

- Desactiva l'usuari anònim.
- Crea un fitxer **index.html** i puja'l mitjançant un client FTP. Finalment, accedeix amb un navegador per comprovar que el servidor configurat i la pàgina web pujada funciona correctament.
- Estableix la/les directives de configuració corresponents perquè sols l'usuari que has configurat puga connectar-se per **FTP** al servidor.
- Activa el **log** i fes una **captura de la sortida** quan un usuari es connecta al servidor i puja i/o baixa un arxiu.

Recorda que, per a poder establir el **document root** d'un servidor virtual d'apache fora del directori `/var/www/` has de permitir-ho expressament en el vhost corresponent. Per fer-ho hauràs d'utilitzar una directiva que ja coneixem aplicada en el vhost corresponent

```
<Directory /home/empresa-client/www/html>
     Options Indexes FollowSymLinks
     AllowOverride None
     Require all granted
</Directory>
```

També hauràs de tenir en compte que l'usuari `www-data` amb el que s'executa apache ha de tenir permisos d'execució en tots els directoris `home` i `empresa-client`.