

Gestión de los servidores FTP

1. El protocolo FTP

FTP (*File Transfer Protocol*) es un protocolo cliente-servidor de transferencia de archivos. Definido en la RFC 114 de 1971, reemplazada por la RFC 959 de 1985, es uno de los protocolos más antiguos de la familia TCP/IP.

Implementado en muchas aplicaciones en el conjunto de los sistemas operativos, y particularmente Linux, sigue siendo muy usado. Sin embargo, necesita una configuración atenta en el servidor, para asegurar un nivel de seguridad suficiente.

Los tres servidores que se tienen que conocer para la certificación LPIC-2 son Pure-FTPd, vsftpd y, de manera menos profunda, ProFTPD.

a. Principios de funcionamiento

El protocolo de aplicaciones FTP se basa en TCP y usa el puerto bien conocido 21 para la transmisión de comandos entre el cliente y el servidor. Los datos se intercambian a través de una segunda conexión TCP con el puerto 20.

FTP puede funcionar en modo anónimo o autenticando los clientes. En este último caso, el cliente tiene que introducir una cuenta de usuario y contraseña válidos para el sistema del servidor. No obstante, el protocolo FTP usa intercambios no cifrados entre el cliente y el servidor, lo que es un problema de seguridad con respecto a la contraseña.

En modo anónimo, los servidores FTP asocian todas las conexiones de los clientes a una cuenta única del sistema, con derechos limitados a lo estrictamente necesario.



El protocolo FTP tiende a ser reemplazado por SFTP (*SSH File Transfer Protocol*), que utiliza comunicaciones cifradas.

b. Modos FTP activo y FTP pasivo

Históricamente, los clientes FTP utilizan el **modo activo**: el cliente envía una solicitud de conexión al servidor, en el puerto TCP 21. Para transferir los datos, el servidor abre una conexión desde el puerto TCP 20, hacia un puerto TCP del cliente, establecido dinámicamente.

Este tipo de funcionamientos puede causar problemas si existe un firewall entre el servidor y el cliente, porque la solicitud de conexión del servidor hacia un puerto dinámico del cliente podría ser bloqueada.

En **modo pasivo**, el cliente efectúa las dos solicitudes de conexión, en el puerto TCP 21 (para intercambio de comandos) y en un puerto dinámico del servidor, especificado al cliente por este último, a través de la conexión de control.

2. Los clientes FTP

Linux dispone de múltiples implementaciones de clientes FTP, en modo línea de comandos y en modo gráfico.

a. Los clientes FTP gráficos

Los clientes FTP en modo gráfico existen para la mayoría de los sistemas operativos. El más conocido es FileZilla, programa open source muy usado en Windows.

b. El cliente FTP en línea de comandos

El comando `ftp` permite lanzar un cliente FTP en modo línea de comandos. El comando es interactivo y usa comandos `ftp` cuyo nombre se parece mucho a los comandos estándar de Linux/Unix.

Sintaxis

```
ftp [IdServidor]
```

El comando solicita una cuenta de usuario y una contraseña. Según la configuración del servidor FTP, puede tratarse de una cuenta de usuario válida en el sistema remoto, o de una cuenta anónima (a menudo `anonymous`) con una contraseña (a menudo `anonymous`).

Si se acepta la conexión, el comando muestra una consola. El usuario puede entonces teclear los comandos `ftp`, para desplazarse en la arborescencia de archivos local o remota, y solicitar transferencias de archivos del servidor al cliente o del cliente al servidor. también puede ejecutar comandos de gestión de archivos en el servidor (supresión, desplazamiento, cambio de nombre, etc.).

Comandos de cliente `ftp` habituales

<code>passive</code>	Fuerza el modo pasivo para la transferencia de datos con el servidor.
<code>pwd</code>	Muestra el directorio actual remoto.
<code>ls</code>	Lista el contenido del directorio actual remoto.
<code>cd</code>	Cambia el directorio actual remoto.
<code>lcd</code>	Cambia el directorio actual local.
<code>get</code>	Copia un archivo remoto hacia el directorio actual local.
<code>mget</code>	Copia varios archivos remotos hacia el directorio actual local.
<code>put</code>	Copia un archivo local hacia el directorio actual remoto.
<code>mput</code>	Copia varios archivos locales hacia el directorio actual remoto.
<code>quit</code>	Final de la conexión.

c. Modo anónimo

En modo anónimo, el cliente FTP especifica la cuenta de usuario `ftp` del servidor, con una contraseña, y el servidor FTP le proporciona un acceso al directorio de conexión de esa cuenta, por defecto `/home/ftp`. Sus derechos de acceso en el sistema del servidor son los atribuidos a esa cuenta.

En general, para conectarse en modo anónimo, hay que teclear el nombre `anonymous` cuando el servidor hace la solicitud de login, y `anonymous` como contraseña (si el servidor solicita una).



En modo anónimo, no está aconsejado autorizar la transferencia de archivos hacia el servidor. Por un lado, como todos los clientes FTP están asociados a la misma cuenta de usuario, existe el riesgo de machacar archivos de otros clientes. Por otro lado, como los clientes son anónimos, algunos podrían usar el servidor para almacenar datos ilegales, esto podría ser responsabilidad del administrador.

d. Modo cuenta usuario

En este modo, el cliente FTP ofrece una cuenta de usuario del sistema del servidor, con una contraseña, y el servidor FTP le da acceso a su directorio de conexión. Sus derechos de acceso en el sistema servidor, son los mismos atribuidos a esta cuenta de usuario.

El intercambio entre el cliente y el servidor se efectúa sin cifrar, incluyendo la contraseña, este modo no está aconsejado por razones de seguridad.

3. El servidor FTP Pure-FTPd

Pure-FTPd es un servidor FTP open source que propone un servicio de transferencia de archivos simple, robusto y eficaz.

a. Opciones de funcionamiento

El daemon `pure-ftpd` funciona por defecto sin archivo de configuración; hay que especificar las opciones deseadas a través de la línea de comandos cuando se lance el servicio.

También podemos especificar en el script de lanzamiento `init System V` o en `systemd` un archivo de configuración, por defecto `/etc/pure-ftpd/pure-ftpd.conf`.

Opciones habituales

<code>--help</code>	Muestra la ayuda.
<code>--displaydotfile</code>	Muestra en el lado del cliente los archivos ocultos (archivos.*).
<code>-anonymousonly</code>	Modo anónimo solamente.
<code>--noanonymous</code>	Imposible de conectarse en modo anónimo.
<code>--anonymouscantupload</code>	Imposible hacer una transferencia de archivos hacia el servidor en modo anónimo.
<code>--anonymouscancreatedirs</code>	Autoriza la creación de directorios por parte de los usuarios anónimos.

Ejemplo

Conexión en modo anónimo a un servidor pure-ftpd:

```
ftp localhost
Trying::1...
```

```

Connected to localhost (::1).
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 14:57. Server port: 21.
220 You will be disconnected after 15 minutes of inactivity.
Name (localhost:root): anonymous
230 Anonymous user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is your current location
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.

```

En modo anónimo, el servidor FTP no solicita ninguna contraseña.

4. El servidor FTP vsftpd

vsftpd (*very secure FTP daemon*) es otro programa de tipo servidor FTP, open source, muy usado en los sistemas Linux. Se trata del servidor FTP por defecto de las distribuciones de tipo Red Hat.

En modo cuenta de usuario, el daemon se basa en la biblioteca PAM para la autenticación de los usuarios, lo que le permite administrar diferentes tipos de cuentas (locales, NIS, LDAP...).

El servidor FTP también puede administrar cuentas de usuario virtuales, cada una con su contraseña y su directorio personal (convertido con chroot en `/var/ftp`), asociadas a la cuenta de usuario del sistema `ftp` (*mapping*), con derechos limitados en el sistema.

a. Configuración del servidor FTP

El daemon carga sus parámetros a través del archivo de configuración `/etc/vsftpd/vsftpd.conf`.

Formato del archivo

parámetro=valor

La mayoría de los parámetros tienen un valor **YES** o **NO**.

Parámetros habituales

<code>anonymous_enable</code>	Autoriza o no el modo anónimo.
<code>local_enable</code>	Autoriza o no a los usuarios a que puedan acceder a su directorio de conexión.
<code>write_enable</code>	Autoriza o no la transferencia de archivos hacia el servidor.
<code>anon_upload_enable</code>	Autoriza o no la transferencia de archivos hacia el servidor en modo anónimo.
<code>anon_mkdir_write_enable</code>	Autoriza o no la creación de directorios en modo anónimo.

b. Lista de usuarios autorizados o rechazados

Podemos especificar cuentas de usuario autorizadas o rechazadas a conectarse al servidor vsftpd. Para ello, las declaramos en un archivo de lista (por defecto `/etc/vsftpd/user_list`).

Siguiendo la configuración del daemon, las cuentas de usuario declaradas en ese archivo no podrán conectarse al servidor FTP o, al contrario, solamente esas cuentas podrán conectarse. Si no tienen derecho a conectarse, el servidor FTP rechazará la conexión, antes incluso de solicitar la contraseña; esta no tendrá que circular de manera inútil y sin cifrar por la red.

Los parámetros de configuración del uso de ese archivo de lista son los siguientes y se encuentran en el archivo `vsftpd.conf` :

Camino de acceso al archivo de tipo lista:

```
userlist_file=/etc/vsftpd/user_list
```

Modo lista de los usuarios autorizados:

```
userlist_enable=YES
```

Modo lista de los usuarios prohibidos:

```
userlist_deny=YES
```

5. El servidor FTP ProFTPD

ProFTPD (*Professional FTP daemon*) es un servidor FTP open source, utilizado frecuentemente en los sistemas Linux. Escrito desde cero, ofrece un alto nivel de configuración y de seguridad.

Su archivo de configuración recoge los principios y el formato del archivo de configuración del servidor HTTP Apache.