

# Practica 1: Servicio FTP

Sergio Paracuellos, Ricardo Muñoz

# Índice

<b>1. Introducción</b>	<b>4</b>
<b>2. Especificaciones</b>	<b>4</b>
2.1. Entorno hardware . . . . .	4
2.2. Entorno software . . . . .	4
2.3. Servidor ftp instalado . . . . .	5
<b>3. Proceso de instalacion</b>	<b>5</b>
<b>4. Arranque del servidor</b>	<b>6</b>
4.1. A través de inetd . . . . .	6
4.2. Como proceso autónomo . . . . .	6
<b>5. Configuración Servidor FTP</b>	<b>6</b>
5.1. Configuracion para Usuarios del Sistema . . . . .	6
5.2. Configuracion para Usuarios Anónimos . . . . .	6
5.2.1. Creacion de cuentas de usuario . . . . .	7
5.2.2. Ficheros y directorios modificados/añadidos . . . . .	7
5.2.3. Configuracion de carga de trabajo . . . . .	8
5.2.4. Archivo de configuración proftpd.conf . . . . .	8
<b>6. Pruebas de Acceso</b>	<b>10</b>
<b>7. Herramientas de medida utilizadas</b>	<b>11</b>

## Índice de figuras

1. Fichero de configuración proftpd.conf . . . . . 10

### 1. Introducción

Antes de comenzar con el comentario del desarrollo de las prácticas queremos introducir en esta sección como hemos planificado las tareas previas para llevar a cabo este proceso.

Hemos montado un servidor de **cv**s para poder realizar la tarea con control de las distintas versiones y poder trabajar cómodamente cada uno en nuestra casa. Hemos modificado el comportamiento de este **cv**s para que cada vez que se produzca un cambio nos lo notifique enviandonos un mail a una lista de correo que hemos montado para este propósito.

También queremos comentar la notación que vamos a seguir de cara a la documentación que nos ocupa.

- **Negrita**: escribiremos en negrita los comandos del sistema, así como el *seteo de variables* y la correspondiente modificación de los archivos del sistema.
- **Cursiva**: escribiremos en cursiva toda función referente a un script, palabras inglesas o similares.

También queremos destacar que aunque las prácticas hayan sido realizadas en un ordenador portatil, hemos instalado en una partición separada una debian estable desde cero y no sobrepasando en ningún caso el tamaño de un disco ZIP. Como editor hemos utilizado **vi**, para no estar en ningún tipo de desventaja respecto a los otros alumnos que realizan las practicas en la sala con un disco ZIP.

Después de estas consideraciones prerealización de las practicas y documentación, pasaremos a analizar cada una de las prácticas propuestas para este bloque.

### 2. Especificaciones

#### 2.1. Entorno hardware

Las características de la maquina de prueba son:

- Procesador Pentium III 1.1 GHz
- Tarjeta de red
- Conexion Telefónica ADSL
- Memoria RAM 512 MB

#### 2.2. Entorno software

Los componentes software que posee la máquina de pruebas son:

- Sistema Operativo: GNU/Linux
- Distribución Debian en su version estable 3.0 (woody)
- Servidor FTP: Pro-ftpd en su version actual 1.2.9

### 2.3. Servidor ftp instalado

Proftpd es un software potente y seguro. Su fichero de configuración utiliza una sintaxis similar a la Apache, lo que permite homogeneizar su configuración. El wu-ftp es probablemente uno de los servidores más difundidos en el sistema Unix por su rendimiento, pero carece de características de servidores bajo Windows. También ha tenido serios problemas de seguridad que han comprometido en alguna ocasión los servidores de empresas.

Proftpd ha sido elegido como servidor ftp oficial por la distribución Debian/GNU Linux. El uso de módulos permite fácilmente extender sus numerosas funcionalidades y por la gran cantidad de programadores que trabajan en él corrigiendo errores. El uso de módulos permite fácilmente extender sus funcionalidades. Existen módulos para:

- Gestión de cuotas (de usuario).
- Otros sistemas de autenticación como LDAP, Mysql, Postgresql...
- Gestión de ratios (por ejemplo, el usuario no puede descargar mas de 1 MB diario).
- Gestión de ancho de banda.

Es por todo esto que hemos elegido el servidor Proftpd.

## 3. Proceso de instalacion

En cuanto a la instalación, y a pesar de ser un paquete disponible en la rama *stable* de debian y accesible mediante apt, hemos optado por bajarnos las fuentes del programa y compilarlo por nuestra cuenta. La version actual y estable de **proftpd** es la *1.2.9* que fue liberada el 31 de Octubre del año 2003.

Para compilar los fuentes, gracias a herramientas como **autotools**, todos los paquetes de fuentes siguen un proceso similar consistente en una serie de pasos que vamos a explicar a continuación:

- Descomprimir el *tar.gz* adquirido de la web y situarnos dentro del directorio que se nos crea al descomprimirlo.
- *./configure*: Lanzamos este script para que verifique las librerías de nuestro sistema de acuerdo a una serie de ficheros escritos por el empaquetador y preparar así un entorno de compilación basado en *Makefiles* que nos automatiza todo el proceso.
- *make*: Este comando es el que realiza la compilación propiamente dicha de todos los ficheros fuentes que componen el programa en cuestión.
- *make install*: Realizará la instalación en nuestro sistema del programa en cuestión recién compilado (ejecutables).

## 4. Arranque del servidor

### 4.1. A través de inetd

Hemos decidido que nuestro servicio ftp arranque automáticamente a través de **inetd**. Para conseguir esto debemos hacer lo siguiente:

- Existe una variable dentro del fichero de configuración global de nuestro ftp (*proftpd.conf*) que toma el nombre de **ServerType** cuyo valor debe establecerse en "inetd".
- Debemos dar de alta el servicio como "servicio a través de inetd" para ellos debemos editar el fichero */etc/inetd.conf* y añadir una línea similar a *ftp stream tcp nowait root /usr/bin/tcpd /usr/local/sbin/proftpd*
- Reiniciar el inetd para que tengan efecto los cambios: */etc/init.d/inetd restart*.

### 4.2. Como proceso autónomo

También tenemos la opción de que arranque como un proceso autónomo, y no seguir ninguno de los tres pasos explicados en el anterior apartado. En este caso, la variable mencionada anteriormente **ServerType** deberá tomar el valor "standalone".

## 5. Configuración Servidor FTP

Una vez en este punto, deberemos tener en cuenta que no es lo mismo una configuración que otra. Vamos a explicarnos; deberemos distinguir que no es lo mismo que el servicio lo utilice un usuario perteneciente al sistema que el resto de usuarios del mundo que queremos que lo usen. Los primeros, al poseer una cuenta en el sistema, accederían a su directorio *home*, mientras que para el resto, se debe proveer un repositorio común del que podrán adquirir los ficheros o paquetes de software que dejemos bajo el mismo. A este tipo de usuarios que acabamos de mencionar los denominaremos usuarios anónimos y deberán utilizar el ftp bajo esa identidad.

### 5.1. Configuración para Usuarios del Sistema

Lo único que nos debe preocupar para esta configuración son los permisos. Debemos tener cuidado, como administradores que somos, que simplemente el usuario registrado en el sistema tiene acceso a su */home*, y por tanto no puede bajarse ficheros que comprometen la seguridad de la máquina como pueden ser */etc/passwd* y */etc/shadow*.

### 5.2. Configuración para Usuarios Anónimos

Es en este punto donde nos vamos a centrar de una manera más detallada.

### 5.2.1. Creación de cuentas de usuario

Vamos a crear un usuario ftp para el uso del ftp anónimo. Para ellos nos ayudamos del comando que posee debian **adduser**. Una vez creado deberemos de modificar el fichero */etc/passwd* de tal forma que no posea cuenta en el sistema. Los cambios pertinentes en */etc/passwd*

- Poner en la columna dos del fichero mencionado del usuario ftp un `*`.
- Quitarle la shell en el sistema cambiando la última columna de */bin/bash* a */bin/false*.

El programa **adduser** nos creará el directorio */home/ftp* que será nuestro directorio de uso anónimo. Dentro de él crearemos los directorios *uploads* y *private* para las operaciones oportunas de los usuarios anónimos.

### 5.2.2. Ficheros y directorios modificados/añadidos

Como hemos comentado, dentro del directorio */home/ftp* residirán todos los archivos que los usuarios anónimos podrán cargar o descargar, con la posibilidad de navegar por ellos de una manera ordenada. Se han creado los siguientes directorios dentro de */home/ftp*:

- *uploads*: En este directorio el usuario anónimo tiene permisos para subir cualquier fichero al servidor. Este directorio posee las siguientes características:
  - Podrá realizar cargas de los ficheros que desee pero no podrá sobrescribir archivos al realizar la carga y no podrá descargar ningún archivo que se encuentre en este directorio. Esto quedará reflejado en el fichero de configuración que mostraremos en la última parte de esta sección.
  - Los permisos asignados a este directorio son 1733 (sticky bit) evitando a los usuarios de la propia máquina listar el directorio */home/ftp/uploads* y conseguir así un servidor de intercambio de ficheros entre usuarios sin los permisos y aprobación del administrador.
- *Downloads*: Este directorio realiza la misma función que el propio */home/ftp*. La diferencia radica en que dentro de */home/ftp* el administrador colocará ficheros sueltos para que se puedan bajar cuando se desee y así el usuario lo localice de una manera rápida y, por el contrario, el directorio */home/ftp/Downloads* permite al administrador la creación de un árbol de directorios donde ordenar los ficheros por temas. Esto se consigue así:
  - Podrá simplemente descargar ficheros del mismo, al contrario que en *uploads*. Esto quedará reflejado en el fichero de configuración que mostraremos en la última parte de esta sección.
  - Los permisos asignados a este directorio son 555, así cualquier usuario no podrá modificar ni eliminar los archivos de este directorio y tampoco podrá crear nuevos.

## 5.2 Configuración para Usuarios Anónimos

---

- *private*: Esto es una zona privada del administrador donde sólo puede decidir que usuario anónimo y que ficheros puede descargarse ya que se trata de archivos ocultos donde un usuario anónimo normal no puede listar ni saber su contenido. Su funcionamiento consiste en que el administrador coloca el archivo oculto en el directorio *private* y avisa al usuario que quiere que se descargue el fichero. Una vez que el usuario conoce el nombre ya puede descargarlo sin problemas. Para configurarlo:
  - Los permisos asignados a este directorio son 1711 (sticky bit) evitando que cualquier usuario de la propia máquina pueda listar contenidos y crear archivos y consiguiendo así un servidor de intercambio de ficheros son permisos del administrador. Esto quedará reflejado en el fichero de configuración que mostraremos en la última parte de esta sección.

### 5.2.3. Configuración de carga de trabajo

El objetivo del administrador de sistemas es, en todo caso, asegurar la estabilidad y seguridad del sistema que administra. Para conseguir un servidor ftp más seguro podemos pulir algunos parámetros dentro de la configuración global de tal forma que obtengamos un mayor control sobre el mismo: número de conexiones, límites en cuanto a ancho de banda...

- Limitar el número de conexiones al servidor: *MaxInstances 30*.
- Limitar el número de conexiones realizadas por un cliente: *MaxInstancePerUser 2*.
- Limitar el ancho de banda por conexión por ejemplo a 1 Kb: *TransferRate RETR 1.0*.
- Limitar el tamaño de ficheros que se transmiten (subida a 200 kb y bajada a 1Gb): *MaxStoreFileSize 200 Kb user ftp* y *MaxRetrieveFileSize 1 Gb*.

### 5.2.4. Archivo de configuración proftpd.conf

El archivo de configuración global tiene el siguiente aspecto:

---

```
# This is a basic ProFTPD configuration file (rename it to
# 'proftpd.conf' for actual use. It establishes a single server
# and a single anonymous login. It assumes that you have a user/group
# "nobody" and "ftp" for normal operation and anon.

ServerName                "ProFTPD ParElk"
ServerType                inetd
DefaultServer             on

# Port 21 is the standard FTP port.
Port                      21

# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
```

10

## 5.2 Configuración para Usuarios Anónimos

---

```
Umask                022

# To prevent DoS attacks, set the maximum number of child processes
# to 30. If you need to allow more than 30 concurrent connections
# at once, simply increase this value. Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd).
MaxInstances         30

#Numero maximo de conexiones por cliente
MaxClientsPerUser   2

#Control de ancho de banda
TransferRate RETR 1.0

#Tamaños maximos de transmision
MaxRetrieveFileSize 1 Gb
MaxStoreFileSize 200 kb user ftp

# Set the user and group under which the server will run.
User                 nobody
Group                nogroup

# To cause every FTP user to be "jailed" (chrooted) into their home
# directory, uncomment this line.
#DefaultRoot ~

# Normally, we want files to be overwriteable.
<Directory />
  AllowOverwrite      on
  AllowStoreRestart   on
  AllowRetrieveRestart on
</Directory>

# A basic anonymous configuration, no upload directories. If you do not
# want anonymous users, simply delete this entire <Anonymous> section.
<Anonymous ~ftp>
  User                 ftp
  Group                ftp
  RequireValidShell    off

# We want clients to be able to login with "anonymous" as well as "ftp"
UserAlias             anonymous ftp

# Limit the maximum number of anonymous logins
MaxClients            10

# We want 'welcome.msg' displayed at login, and '.message' displayed
# in each newly chdired directory.
DisplayLogin          welcome.msg
DisplayFirstChdir     .message

# Limit WRITE everywhere in the anonymous chroot
<Limit WRITE>
  AllowAll
</Limit>
```

```
<Limit READ>
  AllowAll
</Limit>

<Directory uploads>
  <Limit READ>
    DenyAll
  </Limit>
  <Limit STOR WRITE>
    AllowAll
  </Limit>
</Directory>

<Directory private/*>
  <Limit WRITE READ>
    AllowAll
  </Limit>
  <Limit STOR DIRS>
    IgnoreHidden on
    DenyAll
  </Limit>
</Directory>
</Anonymous>
```

80

90

---

Figura 1: Fichero de configuración proftpd.conf

## 6. Pruebas de Acceso

Pruebas de acceso para los usuarios pertenecientes al sistema:

- El usuario no puede salir de su */home*.
- Si se accede a */home/ftp* a través de una cuenta de sistema se observa que no puede modificar ficheros, ni eliminarlos, ni moverlos ni sobrescribirlos.
- Se puede listar los archivos de */home/ftp* y */home/ftp/Downloads* pero no se pueden modificar en ningún caso.
- Si se accede a */home/ftp/uploads* y */home/ftp/private* no se debe ver el contenido de dichos directorios, y aún sabiendo el nombre concreto de cualquier archivo no deberá poderse modificar en ningún caso.
- Dentro de */home/ftp/uploads* el usuario tiene acceso para subir ficheros y modificar sólo aquellos que son de su propiedad. Sin embargo en */home/ftp/private* un usuario desde su cuenta no puede listarlo (como hemos mencionado anteriormente) y necesita permiso del administrador para crear archivos.

Pruebas de acceso para usuarios anónimos:

- Una vez iniciada la sesión ftp, el usuario anónimo no podrá acceder de manera ascendente más allá de su árbol */home/ftp*.
- El usuario no podrá subir ningún archivo a */home/ftp*, ya que esa zona es de descarga de archivos puntuales que nos deje el administrador en un determinado momento.
- El usuario sólo podrá realizar cargas al directorio */home/ftp/uploads* y no podrá modificar ficheros que no sean de su propiedad.
- El usuario no podrá listar ni modificar el contenido del directorio */home/ftp/private* ya que sólo podrá descargar ficheros cuando sepa el nombre concreto de lo que quiere descargar (proporcionado por el administrador).

## 7. Herramientas de medida utilizadas

Para llevar a cabo este propósito hemos utilizado herramientas propias de los sistemas Linux/Unix que controlan el consumo de cpu, memoria ... tales como uptime, ps, top. Estas dos últimas nos permiten una información detallada de cada proceso.