

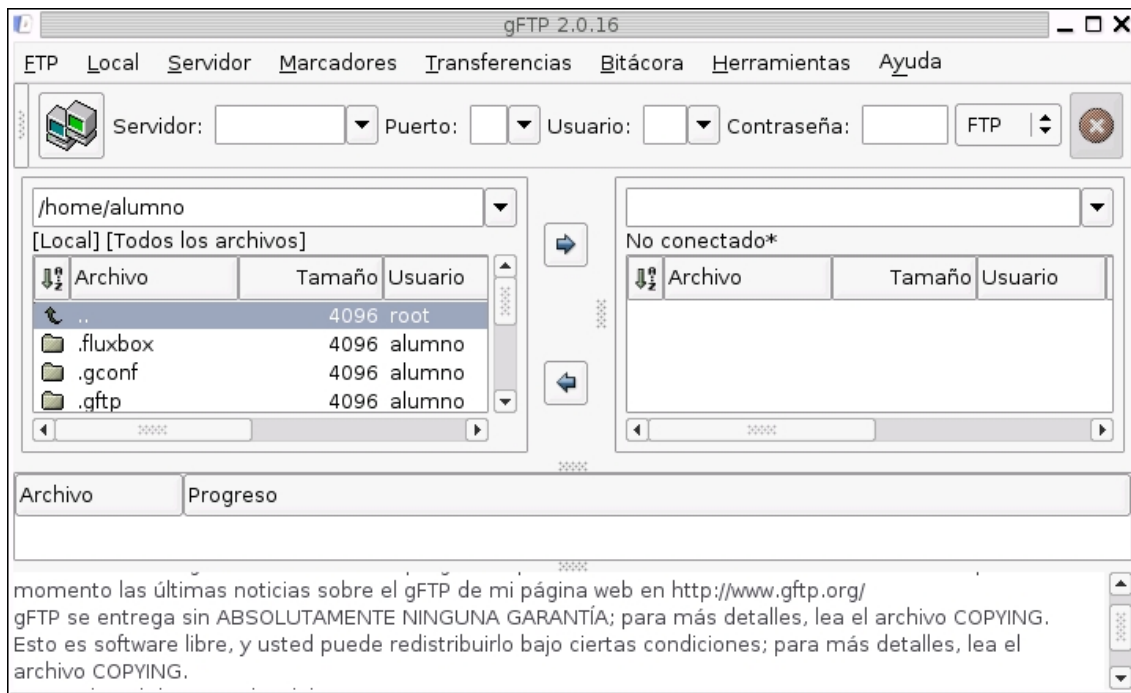
# CAPÍTULO 10

## Configuración de un servidor FTP

El servicio FTP (File Transfer Protocol, o Protocolo de Transferencia de Ficheros) permite que determinados usuarios puedan acceder a determinadas zonas de nuestro servidor donde podrán enviar y coger archivos.

Existen dos formas de utilizar FTP; una de ellas consiste en que los usuarios con cuentas de “shell” accedan a su propio sistema de archivos y carpetas (su directorio en /home) y puedan manipularlo; a esto se le conoce como “acceso FTP autorizado”, ya que el usuario utiliza su nombre de usuario y contraseña. La otra permite que cualquiera se conecte a una sección del sistema de ficheros y cargue o descargue información; esto es lo que se conoce como “acceso FTP anónimo”.

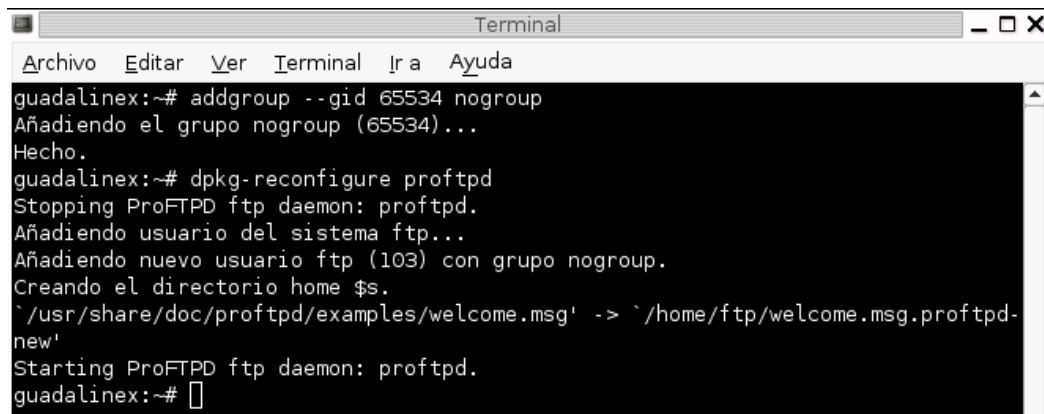
Todas las versiones de Linux vienen desde el principio con un cliente muy sencillo de FTP, llamado “ftp” y se puede utilizar desde la consola; además GuadaLinux dispone de una aplicación gráfica en Aplicaciones -> Internet llamada gFTP, más potente y fácil de utilizar y que se supone sabes manejar (aunque siempre deberías aprender cómo usar el de la consola “por si acaso”). Acude a su página de manual para aprender su funcionamiento.



Existen varios servidores de FTP; hasta hace poco el más utilizado era `wu-ftp`, pero tenía algunos problemas de seguridad; aunque esos problemas se han solventado ha crecido el uso del servidor `ProFTPD`, más sencillo, que además tiene un diseño parecido al de `Apache`. Para instalarlo como de costumbre se puede utilizar `synaptic` o `apt` ("`apt-get install proftpd`"); en ambos casos puede que se instale algún paquete adicional para resolver dependencias.

La única pregunta que nos realizará la instalación es, como el resto de servicios que hemos visto hasta ahora, si queremos ejecutar el demonio de forma independiente ("`Standalone`") o a través del superdaemon `inetd`. Mi consejo es que mientras estés configurándolo lo hagas de forma independiente, ya que puedes evitarte quebraderos de cabeza debidos a problemas de acceso con los "`TCP wrappers`".

En la versión que hemos probado la instalación fallaba debido a que buscaba un grupo que no existía; para solucionarlo debes crear un grupo con el `GID 65534` llamado "`nogroup`"; puedes hacerlo desde la aplicación gráfica o desde la línea de comandos con "`addgroup --gid 65534 nogroup`". Para volver a ejecutar la instalación puedes ejecutar "`dpkg-reconfigure proftpd`".



```
Terminal
Archivo Editar Ver Terminal Ir a Ayuda
guadalinux:~# addgroup --gid 65534 nogroup
Añadiendo el grupo nogroup (65534)...
Hecho.
guadalinux:~# dpkg-reconfigure proftpd
Stopping ProFTPD ftp daemon: proftpd.
Añadiendo usuario del sistema ftp...
Añadiendo nuevo usuario ftp (103) con grupo nogroup.
Creando el directorio home $.
'/usr/share/doc/proftpd/examples/welcome.msg' -> '/home/ftp/welcome.msg.proftpd-
new'
Starting ProFTPD ftp daemon: proftpd.
guadalinux:~#
```

Tras la instalación el demonio se cargará en memoria y estará dispuesto a aceptar conexiones; el archivo de configuración es `/etc/proftpd.conf` y las opciones más relevantes que presenta son:

|                |                                                                 |
|----------------|-----------------------------------------------------------------|
| ServerName:    | Nombre del servidor (el que aparece cuando te conectas).        |
| ServerType:    | Modo de funcionamiento (standalone o inetd).                    |
| ShowSymlinks   | Muestra los enlaces simbólicos para que sean accedidos.         |
| AllowOverwrite | Permite la escritura, es decir, subir o borrar archivos.        |
| DisplayLogin   | Mensaje de bienvenida (está en <code>/home/ftp</code> ).        |
| Port           | Puerto para escuchar conexiones entrantes (por defecto el 21).  |
| MaxInstances   | Número máximo de conexiones simultáneas (sólo standalone).      |
| User/Group     | Usuario/grupo para ejecutar el demonio (nobody/nogroup).        |
| Umask          | Permisos que tendrán los archivos subidos.                      |
| AllowOverwrite | Indica si archivos existente pueden ser sobreescritos (on/off). |

Al igual que Apache pueden definirse directivas sobre directorios; por ejemplo siempre aparece la siguiente, que establece los permisos `rw-r--r--` para los nuevos archivos, y permite que los archivos sean sobreescritos por los nuevos.

```
<Directory /*>
    Umask 022
    AllowOverwrite on
</Directory>
```

Si queremos habilitar el acceso anónimo debemos definir una directiva `<Anonymous ~ftp>`, donde especificar el usuario/grupo de este usuario además de otras opciones; un caso típico sería :

```
<Anonymous ~ftp>
    User          ftp
```

```
Group          nogroup
UserAlias              anonymous ftp
RequireValidShell  off
MaxClients        10
DisplayLogin              welcome.msg
DisplayFirstChdir  .message
```

```
<Directory *>
    <Limit WRITE>
        DenyAll
    </Limit>
</Directory>
```

</Anonymous>

Esto permitirá a usuarios anónimos con nombre de usuario “ftp” o “anonymous” acceder para leer los archivos, pero no para escribir, debido a la directiva “Limit WRITE”. Los usuarios no tienen por qué tener cuenta en nuestro sistema al estar “RequireValidShell” a “off”. También se limita el número de accesos anónimos a 10.

El directorio inicial para este tipo de accesos es /home/ftp, ya que durante la instalación se creó un usuario (sin “shell”, puedes comprobarlo) llamado “ftp”, siendo éste su directorio principal.

Si además queremos que estos usuarios puedan subir archivos, habría que añadir antes de cerrar la directiva <Anonymous>:

```
<Directory incoming>
    <Limit READ WRITE>
        DenyAll
    </Limit>
    <Limit STOR>
        AllowAll
    </Limit>
</Directory>
```

Para que esto funcione debes crear el directorio /home/ftp/incoming y ponerle los permisos apropiados:

```
# mkdir /home/ftp/incoming
# chown ftp:nogroup /home/ftp/incoming
```

## ***Ejercicios***

- 1) Limita el número de conexiones simultáneas a 10; activa el acceso anónimo para lectura y escritura y limita el número de estas conexiones a 4.
- 2) Modifica la configuración anterior para eliminar el acceso anónimo de escritura.

### **Soluciones**

- 1) Tan sólo debes repetir el ejemplo propuesto y modificar las opciones:  
MaxInstances        10  
MaxClients         4
- 2) Elimina (o mejor añade delante de cada línea el símbolo "#") la sección <Directory incoming>