



**Instituto Politécnico
Nacional**

**Escuela Superior de
Cómputo**



Administración de Servicios en Red

Profesor:

Soto Ramos Manuel Alejandro

Alumnos:

Dominguez de la Rosa Bryan

Pacheco Díaz Fernando Jair

Vivia Delgadillo Rocío

Grupo:

4CV3

**Instalación y Configuración del Servidor y
Clientes FTP**

Protocolo FTP	3
Servidor PROFTPD	3
Instalación	3
Configuración	4
Restricciones	6
Seguridad	7
FTPS	7
SFTP	10
Configuración de bitácora	12
Clientes	14
FileZilla	14
Terminal	14
Navegador	15
Aplicación Móvil	15
Referencias	17

Protocolo FTP

El protocolo de transferencia de archivos (FTP) es uno de los protocolos más viejos y populares que se encuentran en la Internet hoy día. Su objetivo es el de transmitir archivos exitosamente entre máquinas en una red.

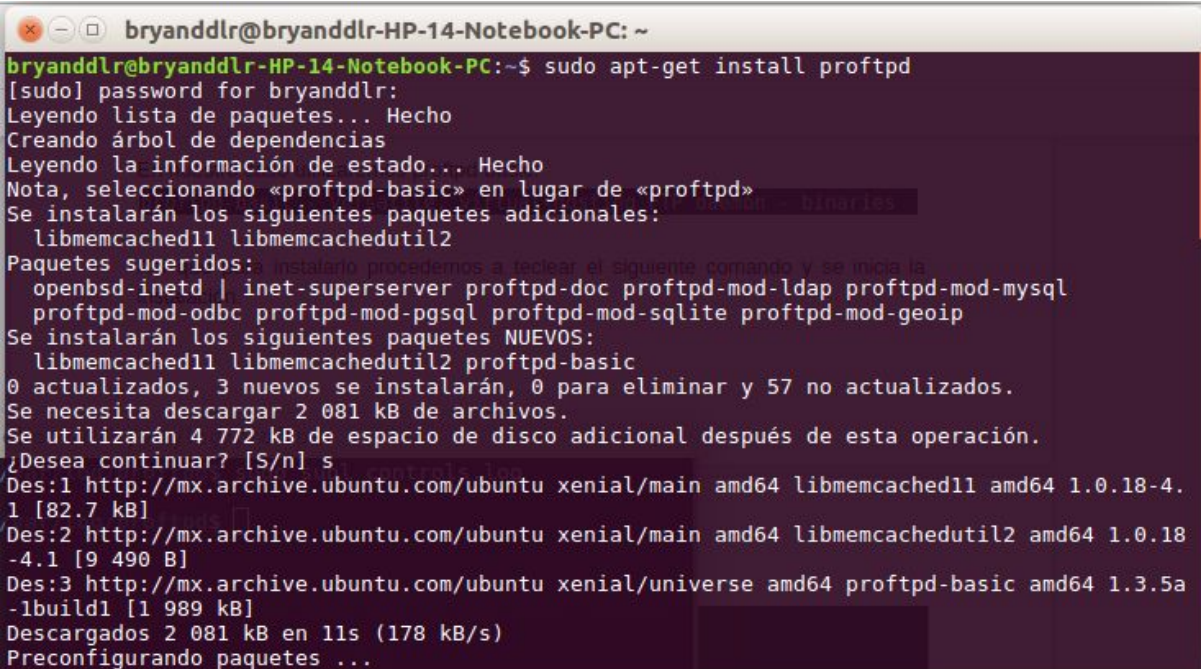
FTP utiliza una arquitectura cliente/servidor para transferir archivos usando el protocolo de red TCP. [1]

Servidor PROFTPD

EL servidor elegido para montar nuestro protocolo FTP es el servidor Proftpd, el cual fue escrito para ser usado en Unix y sus diferentes distribuciones, no existe soporte nativo del servidor sobre Windows. [2]

Instalación

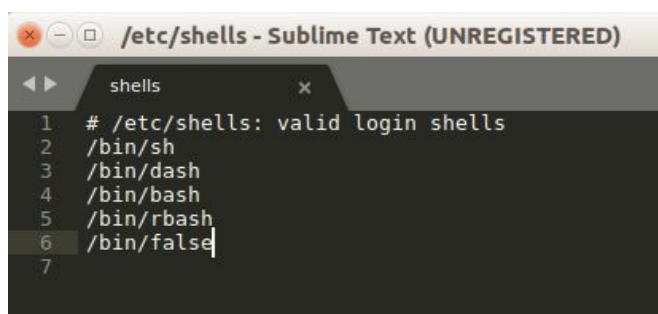
Ejecutamos el comando **\$sudo apt-get install proftpd**, se nos preguntará si deseamos instalar el servidor de manera independiente o sobre inetd, elegiremos la opción **independiente**.



```
bryanddlr@bryanddlr-HP-14-Notebook-PC: ~  
bryanddlr@bryanddlr-HP-14-Notebook-PC:~$ sudo apt-get install proftpd  
[sudo] password for bryanddlr:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Nota, seleccionando «proftpd-basic» en lugar de «proftpd»  
Se instalarán los siguientes paquetes adicionales:  
  libmemcached11 libmemcachedutil2  
Paquetes sugeridos: openbsd-inetd | inet-superserver proftpd-doc proftpd-mod-ldap proftpd-mod-mysql  
  proftpd-mod-odbc proftpd-mod-pgsql proftpd-mod-sqlite proftpd-mod-geoip  
Se instalarán los siguientes paquetes NUEVOS:  
  libmemcached11 libmemcachedutil2 proftpd-basic  
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 57 no actualizados.  
Se necesita descargar 2 081 kB de archivos.  
Se utilizarán 4 772 kB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] s  
Des:1 http://mx.archive.ubuntu.com/ubuntu xenial/main amd64 libmemcached11 amd64 1.0.18-4.  
1 [82.7 kB]  
Des:2 http://mx.archive.ubuntu.com/ubuntu xenial/main amd64 libmemcachedutil2 amd64 1.0.18  
-4.1 [9 490 B]  
Des:3 http://mx.archive.ubuntu.com/ubuntu xenial/universe amd64 proftpd-basic amd64 1.3.5a  
-1build1 [1 989 kB]  
Descargados 2 081 kB en 11s (178 kB/s)  
Preconfigurando paquetes ...
```

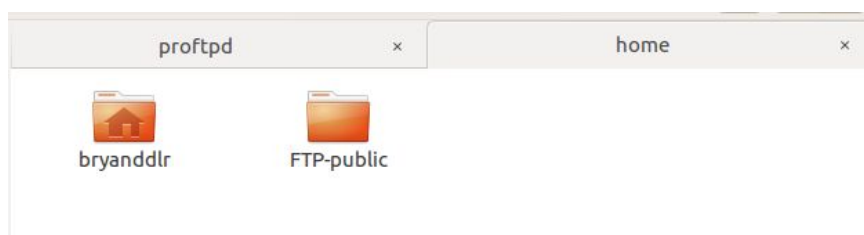
Configuración

Crearemos un shell falso para que los usuarios que accedan al servidor no puedan acceder a la línea de comandos del equipo. Abrimos el archivo ubicado en **/etc/shells** y agregamos el shell falso.



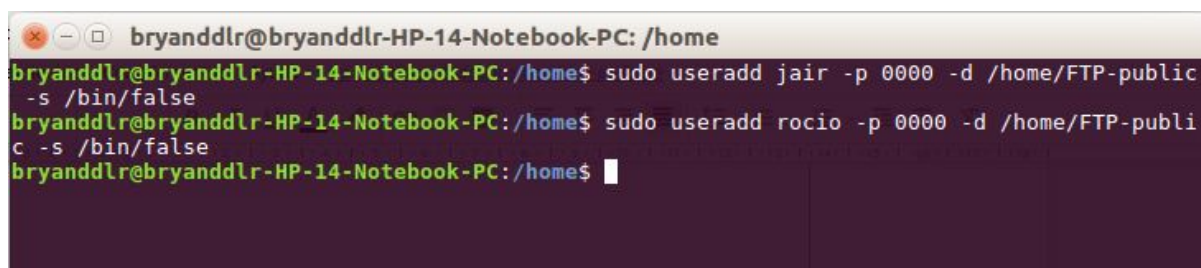
```
1 # /etc/shells: valid login shells
2 /bin/sh
3 /bin/dash
4 /bin/bash
5 /bin/rbash
6 /bin/false
7
```

A continuación creamos una carpeta que será el home de los usuarios del servidor. Esta carpeta será la utilizada para la interacción con los archivos. Para eso nos vamos a la ubicación **/home** y mediante el comando **\$sudo mkdir FTP-public** creamos el directorio.



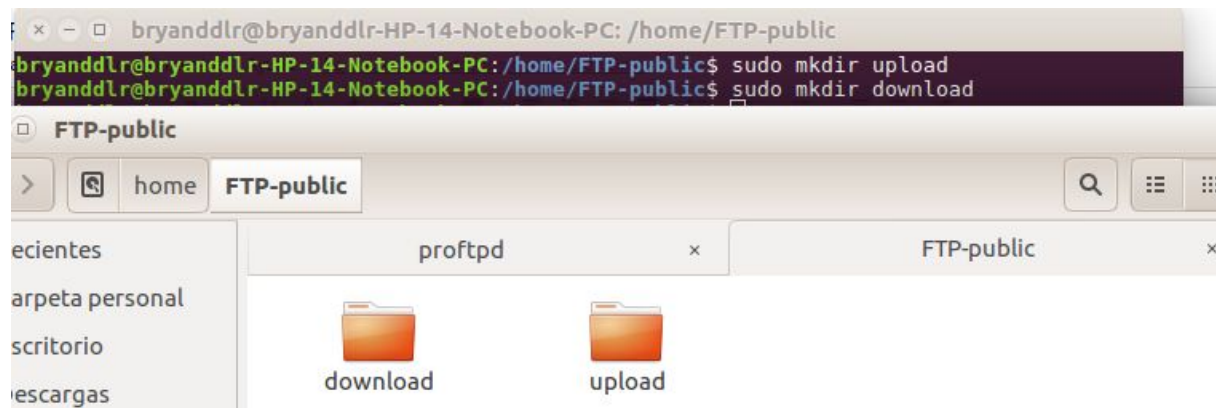
El siguiente paso es dar de alta usuarios que podrán hacer uso del servidor, para ello utilizamos el comando

\$sudo useradd <USER> -p <PASSWORD> -d <HOME_DIR> -s <SHELL>

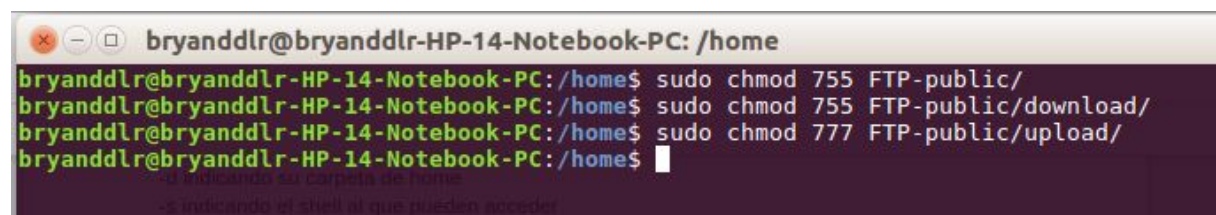


```
bryanddlr@bryanddlr-HP-14-Notebook-PC: /home
bryanddlr@bryanddlr-HP-14-Notebook-PC:/home$ sudo useradd jair -p 0000 -d /home/FTP-public -s /bin/false
bryanddlr@bryanddlr-HP-14-Notebook-PC:/home$ sudo useradd rocio -p 0000 -d /home/FTP-public -s /bin/false
bryanddlr@bryanddlr-HP-14-Notebook-PC:/home$
```

El siguiente paso es crear los directorios de carga y descarga de archivos, dentro del directorio FTP-public creado previamente



Y se les asignan a dichas carpetas los correspondientes permisos de escritura y lectura para que puedan ser utilizados de la manera correcta.



Ahora procedemos a editar el archivo de configuración del servidor, el cual se encuentra en **/etc**. La configuración por defecto es efectiva, pero los cambios realizados para personalizar se pueden ver a continuación

```

10 # Set off to disable IPv6 support which is annoying on IPv4 only boxes.
11 # UseIPv6 on
12 # If set on you can experience a longer connection delay in many cases.
13 IdentLookups off
14
15 ServerName "Debian"
16 # Set to inetd only if you would run proftpd by inetd/xinetd.
17 # Read README.Debian for more information on proper configuration.
18 ServerType standalone
19 DeferWelcome off
20
21 MultilineRFC2228 on
22 DefaultServer on
23 ShowSymlinks on
24
25 TimeoutNoTransfer 600
26 TimeoutStalled 600
27 TimeoutIdle 1200
28
29 DisplayLogin welcome.msg
30 DisplayChdir .message true
31 ListOptions "-l"
32
33 DenyFilter \*./
34
35 # Use this to jail all users in their homes
36 DefaultRoot /home/public_FTP
37 #DefaultRoot ~
38
39 # Users require a valid shell listed in /etc/shells to login.
40 # Use this directive to release that constrain.
41 # RequireValidShell off

```

Restricciones

La configuración de las restricciones de acceso al recurso se realizan en el archivo proftpd.conf, ubicado en /etc/proftpd/, podemos acceder a éste de la siguiente forma:

```
$ sudo cd /etc/proftpd/proftpd.conf
```

A continuación, se indican las directivas necesarias según la restricción que se requiera, dichas directivas se especifican en el directorio en el cual se están colocando las restricciones.

- Para **restringir acceso al recurso por dirección IP del cliente** usaremos la directiva **Limit** de la siguiente forma:

```
<Limit LOGIN>
    Order deny, allow
    Deny from direcciónIPRestringida
    AllowAll
</Limit>
```

- Para **restringir acceso al recurso por usuario** de igual forma usaremos la directiva **Limit**:

```
<Limit LOGIN>
    DenyUser nombreUsuario
    DenyAll
</Limit>
```

Algunos otros parámetros son: **AllowUser** que permite el acceso a un usuario específico y **DenyAll** bloquea el acceso a todos los usuarios excepto a los especificados con AllowUser.

- Para **restringir acceso al recurso por grupo de usuarios** nuevamente con la directiva Limit:

```
<Limit LOGIN>
    DenyGroup nombreGrupo
</Limit>
```

El parámetro para permitir acceso a un grupo determinado es **AllowGroup**.

Para restringir por directorios específicos, como que no se puedan subir archivos a uno en especial o que no puedan entrar todos a una carpeta en específico, se utilizan la directiva directory:

```
<Directory /home/public_FTP>
    Umask      022 022
    AllowOverride off

    <Limit MKD STOR DELE XMKD RNRF RNT0 RMD XRMD>
        Deny All
    </Limit>
</Directory>

<Directory /home/public_FTP/download/*>
    Umask      022 022
    AllowOverride off

    <Limit MKD STOR DELE XMKD RNRF RNT0 RMD XRMD>
        Deny All
    </Limit>
</Directory>

<Directory /home/public_FTP/upload/*>
    Umask      022 022
    AllowOverride on

    <Limit READ RMD DELE>
        Deny All
    </Limit>

    <Limit STOR CWD MKD>
        AllowAll
    </Limit>
</Directory>
```

Seguridad

Existen 2 maneras de crear una conexión “segura” utilizando FTP, una es con certificados SSL utilizando el llamado FTPS y otra con una llave SSH al cual se le llama SFTP, este último es el más utilizado pues es considerado más seguro.

FTPS

Se utilizan certificados SSL que con la herramienta openssl podemos generar uno aunque no sea reconocido a primera instancia por un tercero, pero le da información al cliente de quien trata de hacer la conexión. Para realizarlo solo se sigue lo siguiente.

Utilizando openssl se crea un certificado autofirmado que tendrá información básica de quien lo firma, en la línea se especifica el número de días de validez de dicho certificado y donde se colocarán los archivos de salida.

```
jair@lap-jair:~$ sudo openssl req -x509 -nodes -newkey rsa:2048 -keyout /etc/ssl/private/proftpdserverkey.pem -out /etc/ssl/certs/proftpdcertificate.pem -days 365
Generating a 2048 bit RSA private key
..+++
.....+++
writing new private key to '/etc/ssl/private/proftpdserverkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:Mexico City
Locality Name (eg, city) []:Gustavo A Madero
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ESCOM IPN
Organizational Unit Name (eg, section) []:Equipo 9 Redes 3
Common Name (e.g. server FQDN or YOUR name) []:FTP server
Email Address []:
jair@lap-jair:~$
```

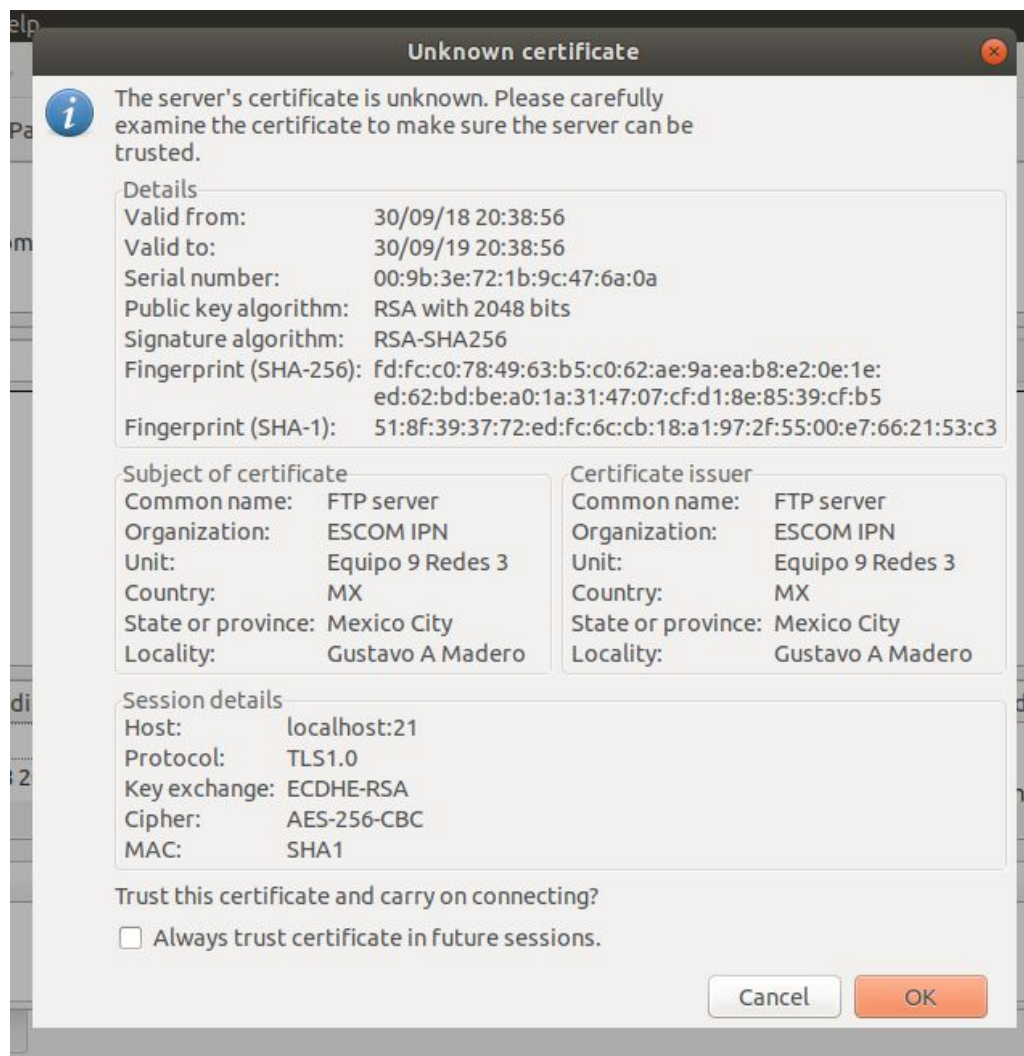
Posteriormente se crea (O modifica si ya está hecho) el archivo de configuración tls.conf, nótese que las líneas comentadas se dejan por referencia al original y se agregan las líneas 11 a 18 de la imagen.

```
tls.conf
1 #
2 # Proftpd sample configuration for FTPS connections.
3 #
4 # Note that FTPS impose some limitations in NAT traversing.
5 # See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.html
6 # for more information.
7 #
8
9 <IfModule mod_tls.c>
10
11 TLSRSCertificateFile /etc/ssl/certs/proftpdcertificate.pem
12 TLSRSCertificateKeyFile /etc/ssl/private/proftpdserverkey.pem
13 TLSEngine on
14 TLSLog /var/log/proftpd/tls.log
15 TLSProtocol SSLv23
16 TLSRequired on
17 TLSOptions NoCertRequest EnableDiags NoSessionReuseRequired
18 TLSVerifyClient off
19
20 #TLSEngine on
21 #TLSLog /var/log/proftpd/tls.log
22 #TLSProtocol SSLv23
23 #
24 # Server SSL certificate. You can generate a self-signed certificate using
25 # a command like:
26 #
```


Posteriormente se descomenta (O se escribe) la inclusión del archivo tls en el proftpd.conf

```
130
131 #
132 # Alternative authentication frameworks
133 #
134 #Include /etc/proftpd/ldap.conf
135 #Include /etc/proftpd/sql.conf
136
137 #
138 # This is used for FTPS connections
139 #
140 Include /etc/proftpd/tls.conf
141
```

Y finalmente, en cualquier cliente le especificamos que será una conexión con ftps y debería detectarla y mostrar el certificado para escoger si se confía o no en este.



SFTP

Esta opción es más confiable y ampliamente más utilizada que FTPS hoy en día, utiliza SSH y para poder configurarlo se hace lo siguiente. Creamos un nuevo archivo de configuración.

```
jair@lap-jair:/etc/proftpd/conf.d$ sudo subl sftp.conf
```

Y lo llenamos de la siguiente manera

```
sftp.conf x proftpd.conf x
1 <IfModule mod_sftp.c>
2
3     SFTPEngine on
4     Port 2222
5     SFTPLog /var/log/proftpd/sftp.log
6
7     # Configure both the RSA and DSA host keys, using the same host key
8     # files that OpenSSH uses.
9     SFTPHostKey /etc/ssh/ssh_host_rsa_key
10    SFTPHostKey /etc/ssh/ssh_host_dsa_key
11
12    SFTPAuthMethods publickey
13
14    SFTPAuthorizedUserKeys file:/etc/proftpd/authorized_keys/%u
15
16    # Enable compression
17    SFTPCompression delayed
18
19 </IfModule>
```

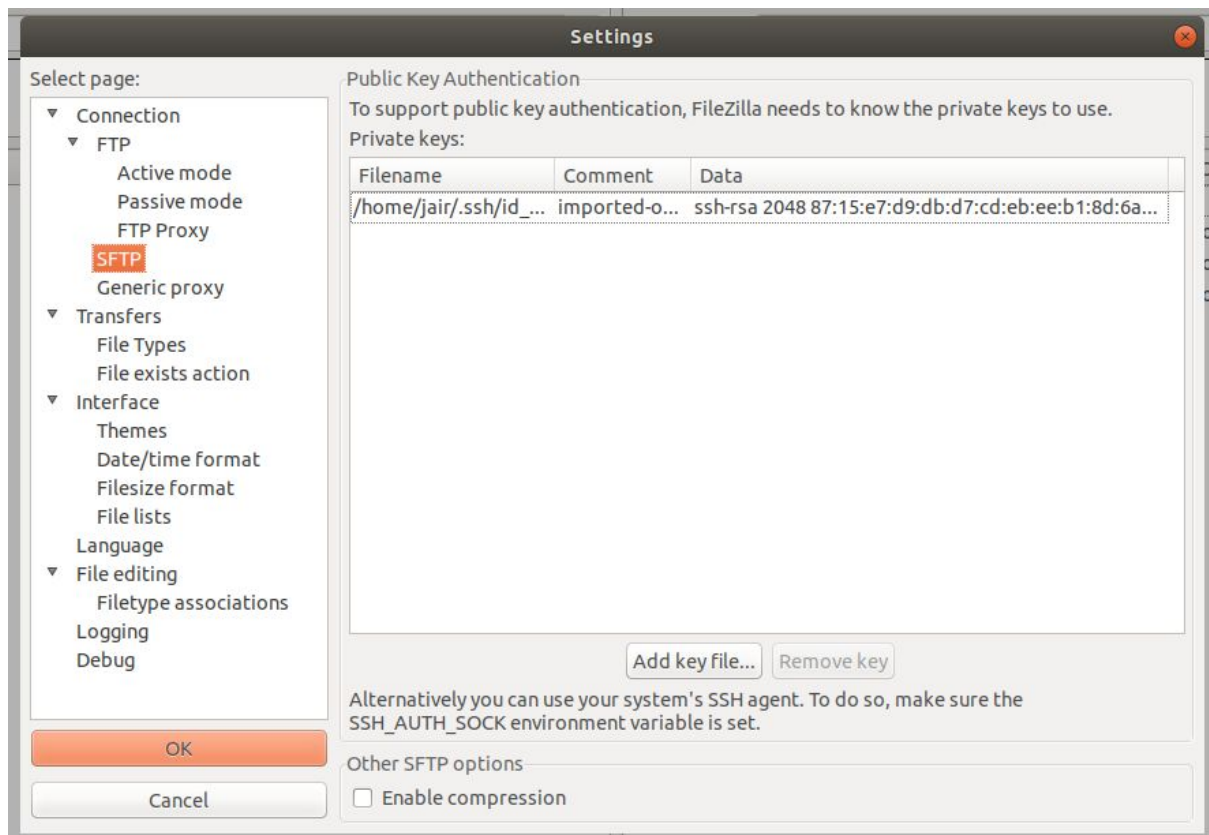
Creamos un directorio para las llaves

```
jair@lap-jair:~$ sudo mkdir /etc/proftpd/authorized_keys
```

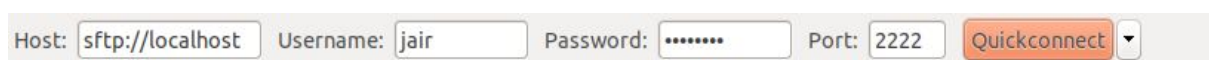
Y convertimos las llaves que usaremos en el servidor, para un usuario se sigue el siguiente comando.

```
jair@lap-jair:~/ssh$ ssh-keygen -e -f ~/jair/.ssh/authorized_keys | tee /etc/pro
ftpd/authorized_keys/jair
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted by jair@lap-jair from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAQDNwX1XTTKiLGC54A22AEKF669VYLrRmUmYBq7B/Q
AwtoGzNxypmzgBMzpEP91ZD+r9b3e7hsA1HQJ7QFacHkY0diNlfeNgxdBkcwVEecrw5/z
ZSIWzPG/UZtQ7G5uw30kjQZMjZvNFi32CeS87uiIRCenRizC8+/EirPpCYV4qLL3tNu50i
m7iOegwbDeLZeqBeov4Dmh3oR/RGvVKErLR9sMfXhtqTUEtrl9udIDLz7Gh01QaSaD2pfQ
zj5EY8jSt1kvCbSL/If6BmfUNqyNqu+UkSv7uKaJCSGhCNC4j3BJVpp1nScmnY9+bCZfbk
GRwYF4Qv4nEjLRdfOyl0X5
---- END SSH2 PUBLIC KEY ----
```

Todo esto considerando que ya est[ame] montado SSH en el servidor y que se cuenta con las llaves tanto el usuario como del propio servidor. Modificamos el cliente de tal manera que le demos la llave p[ub]lica del usuario que va a acceder con sftp



Despu[es] ingresamos al servidor especificando que ser[ame] por sftp y utilizando el puerto que modificamos en el archivo de configuraci[on].



Finalmente nos pedir[ame] revisar la llave del host, para verificar que sea la correcta.



Configuración de bitácora

Por default, el servidor proftpd genera 3 archivos de bitácora:

- proftpd.log
- controls.log
- xferlog

Sin embargo, podemos crear archivos personalizados activando las banderas que necesitemos y estableciendo la directiva LogFormat en el archivo proftpd.conf [4].

Una vez generado el formato que necesitemos, usamos la directiva ExtendedLog para establecer una ruta donde se guardará el archivo personalizado y elegimos qué operaciones queremos que registre, en nuestro caso registramos todas las banderas.

Se agregaron las directivas al archivo proftpd.conf:

```
LogFormat custom "%a %u %t %m %f %s %b"  
TransferLog /var/log/proftpd/xferlog  
SystemLog /var/log/proftpd/proftpd.log  
ExtendedLog /var/log/proftpd/custom.log ALL custom
```

Otra opción que nos brinda el servidor proftpd es decidir que nivel de mensajes vamos a guardar. La siguiente tabla muestra los niveles de mensaje implementados en el servidor:

Level	Description
EMERG	Fatal/unrecoverable error/condition, application is unusable and stops immediately
ALERT	Condition requires immediate intervention by administrator/operator
CRIT	Condition should be corrected immediately, but indicates <i>e.g.</i> failure in secondary system/library
ERR	Non-urgent failure conditions that should be relayed to developers and/or administrators; should be resolved/corrected soon
WARNING	Unexpected error/condition that <i>may</i> require intervention to review/correct
NOTICE	Significant/noteworthy condition, no intervention/action required
INFO	Normal operating conditions, no intervention/action required
DEBUG	Internal details of application operations useful to developers, not necessarily useful during normal operations

Los niveles están ordenados descendentemente por prioridad. Por default el servidor guarda todos los niveles de mensajes. Si queremos guardar solo a partir de cierto nivel, se utiliza la directiva **SyslogLevel**, cuya sintaxis es:

SyslogLevel <LEVEL>

Donde <LEVEL> será el nivel mínimo que se guardará en las bitácoras.

Para la generación de resúmenes se utilizó el lenguaje de programación python en su versión 2.7. Se eligió este lenguaje debido a la sencillez en que se puede realizar el manejo de ficheros (en este caso, los archivos log), además de que cuenta con diversos paquetes que permiten dar un formato presentable a los datos de salida.

Para instalar python en nuestro sistema operativo Ubuntu necesitamos ejecutar las siguientes líneas en la consola:

\$sudo apt update

\$sudo apt install python2.7 python-pip

```
bryanddlr@bryanddlr-HP-14-Notebook-PC:~$ sudo apt install python2.7 python-pip
[sudo] password for bryanddlr:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
python2.7 ya está en su versión más reciente (2.7.12-lubuntu0~16.04.3).
Se instalarán los siguientes paquetes adicionales:
  libexpat1-dev libpython-all-dev libpython-dev libpython2.7-dev python-all
  python-all-dev python-dev python-pip-whl python-pkg-resources python-setuptools
  python-wheel python2.7-dev
Paquetes sugeridos:
  python-setuptools-doc
Se instalarán los siguientes paquetes NUEVOS:
  libexpat1-dev libpython-all-dev libpython-dev libpython2.7-dev python-all
  python-all-dev python-dev python-pip python-pip-whl python-pkg-resources
  python-setuptools python-wheel python2.7-dev
0 actualizados, 13 nuevos se instalarán, 0 para eliminar y 41 no actualizados.
Se necesita descargar 29.8 MB de archivos.
Se utilizarán 45.2 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Una vez teniendo python en nuestro sistema operativo, necesitamos descargar un paquete que nos permitirá dar formato de tabla a nuestros datos de salida. El paquete mencionado se llama tabulate y se descarga con las siguientes líneas:

\$pip install tabulate

Los resúmenes realizan un filtro a la bitácora personalizada por usuario y por operación realizada. El script del resumen se ejecuta de la siguiente manera:

\$python filter.py <logFile> <user> <operation>

Donde:

- <logFile> es el nombre del archivo personalizado de bitácora
- <user> es el nombre del usuario del cual queremos saber sus operaciones.
- <operation> es un número entero que va de 1 a 4:
 - 1: Los archivos o carpetas que ha subido el usuario
 - 2: Los archivos que ha descargado el usuario
 - 3: Los archivos o carpetas que ha borrado el usuario
 - 4: Los archivos o carpetas que ha renombrado el usuario

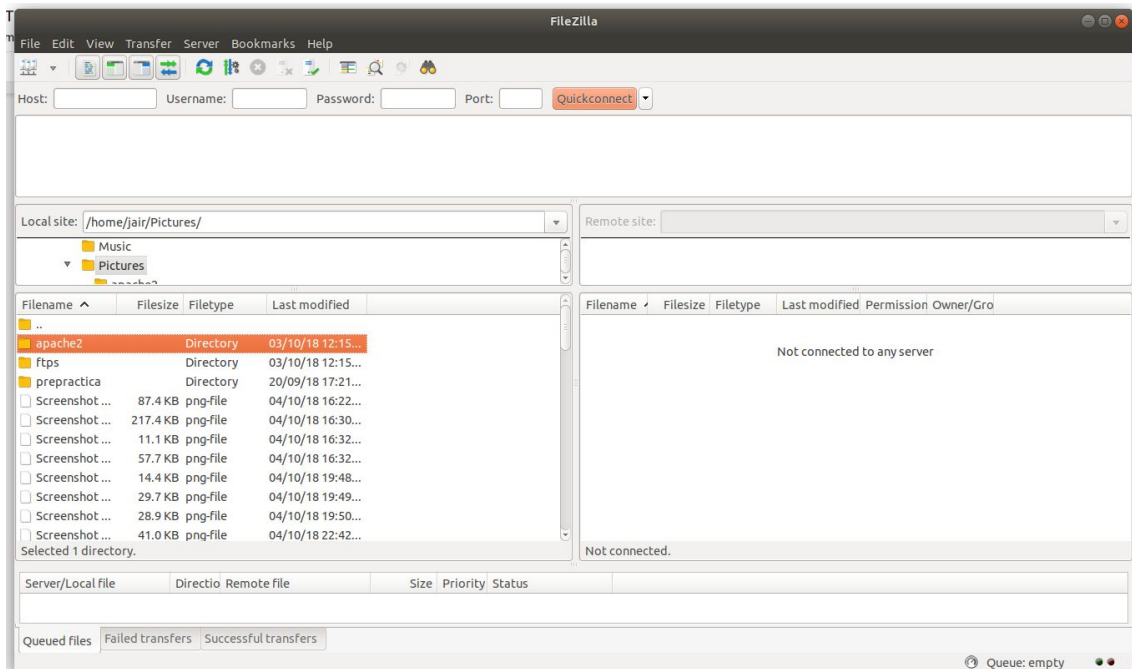
Cientes

FileZilla

Es el cliente FTP gráfico más utilizado, puede ser usado para más que FTP y tiene métodos de configuración muy intuitivos y seguros. Se ejecuta lo siguiente para instalarlo.

```
$ sudo apt install filezilla
```

Y ejecutarlo solo poniendo su nombre en la consola.



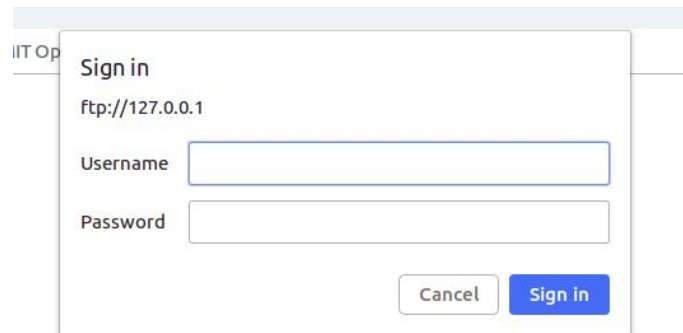
Terminal

Existe un comando para utilizar un cliente FTP: `ftp nombreHost`, el cual nos permite acceder al servidor y navegar utilizando comando escrito, los cuales se pueden revisar en su manual respectivo.

```
jair@Lap-jair:~$ ftp 192.168.100.9
Connected to 192.168.100.9.
220 ProFTPD 1.3.5e Server (Debian) [::ffff:192.168.100.9]
Name (192.168.100.9:jair): jair
331 Password required for jair
Password:
230 User jair logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x  2 root    root      4096 Oct  5 03:42 download
-rw-r--r--  1 root    root       14 Oct  3 16:17 test.txt
drwxrwxrwx  2 root    root      4096 Oct  6 01:18 upload
226 Transfer complete
```

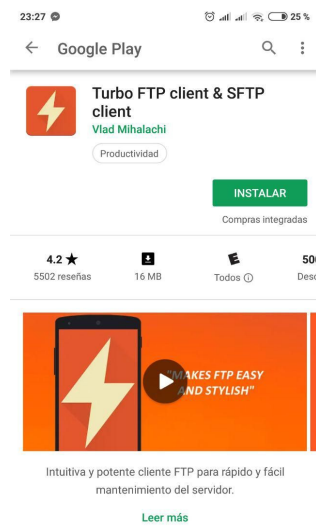
Navegador

La mayoría de los navegadores actuales soportan conexión FTP, basta con poner `ftp://nombreHost.com` para poder acceder al directorio y ver o bajar archivos, la limitación principal es que por defecto no se podrían subir archivos.

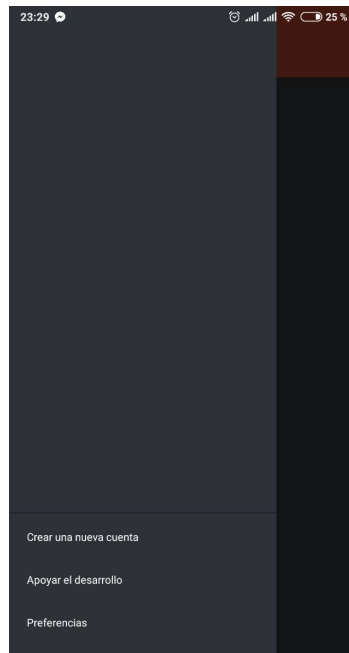


Aplicación Móvil

La aplicación **Turbo FTP client and SFTP client** permite realizar una conexión a un servidor FTP. Se utilizó en Android, descargando desde la playstore:



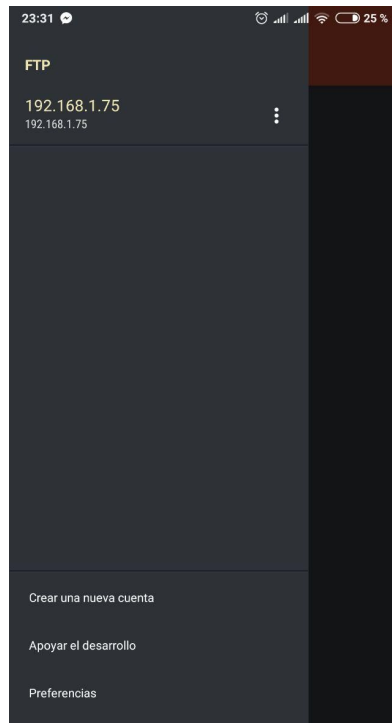
Una vez instalada, tenemos que crear una nueva cuenta y seleccionar si queremos FTP o SFTP:



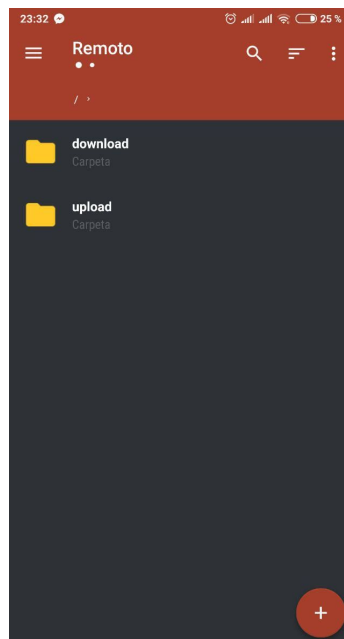
El nombre de la conexión y el servidor serán la IP de nuestro servidor FTP, el usuario debe estar registrado y la contraseña debe ser correcta. Presionamos el icono guardar:

A screenshot of the 'Crear una nueva cuenta' (Create a new account) form in a mobile application. The form has a dark gray background with white text. At the top, there is a red header bar with a back arrow, the title 'Crear una nueva cuenta', and two icons (a square and a gear). Below the header, the form is divided into two sections: 'General' and 'Avanzado'. The 'General' section contains five input fields: 'Nombre de la conexión' (filled with '192.168.1.75'), 'Usuario' (filled with 'bryan'), 'Contraseña' (filled with dots), 'Servidor' (filled with '192.168.1.75'), and 'Puerto' (filled with '21'). The 'Avanzado' section contains one visible input field: 'Raíz' (empty). The 'Avanzado' section is partially obscured by a black bar at the bottom of the screen.

Una vez creada la cuenta, iniciamos sesión dando clic en ella:



Al validar el login, ya podemos tener acceso a las carpetas de upload y download:



Referencias

[1] <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ftp.html>

[2] <http://www.proftpd.org/docs/faq/faq.pdf>

[3] <https://www.thegeekslearn.com/how-to-configure-sftp-in-proftpd/>

[4] http://proftpd.org/docs/directives/linked/config_ref_LogFormat.html

[5] http://proftpd.org/docs/directives/linked/config_ref_ExtendedLog.html