



# Despliegue de aplicaciones web

Javier Muñoz Carmona

```
mirror_mod.use_z = False
elif_operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add back the
mirror_op.select=1
modifier_op.select=1
copy.context.scene.objects.active = modifier_op
print("Selected" + str(modifier_op)) # m
```



# **D**espliegue de aplicaciones web

Consulte nuestra página web: [www.sintesis.com](http://www.sintesis.com)  
En ella encontrará el catálogo completo y comentado



Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de la propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (arts. 270 y sigs. Código Penal). El Centro Español de Derechos Reprográficos ([www.cedro.org](http://www.cedro.org)) veila por el respeto de los citados derechos.

# Despliegue de aplicaciones web

Javier Muñoz Carmona



ASESOR EDITORIAL:  
Juan Carlos Moreno Pérez

© Javier Muñoz Carmona

© EDITORIAL SÍNTESIS, S. A.  
Vallehermoso, 34. 28015 Madrid  
Teléfono 91 593 20 98  
<http://www.sintesis.com>

ISBN: 978-84-1357-070-9  
Depósito Legal: M-2.884-2021

Impreso en España - Printed in Spain

Reservados todos los derechos. Está prohibido, bajo las sanciones penales y el resarcimiento civil previstos en las leyes, reproducir, registrar o transmitir esta publicación, íntegra o parcialmente, por cualquier sistema de recuperación y por cualquier medio, sea mecánico, electrónico, magnético, electroóptico, por fotocopia o por cualquier otro, sin la autorización previa por escrito de Editorial Síntesis, S. A.

# índice

<b>PRESENTACIÓN .....</b>	9
<b>1. SERVICIOS DE RED IMPLICADOS EN EL DESPLIEGUE DE UNA APLICACIÓN .....</b>	11
Objetivos .....	11
Mapa conceptual .....	12
Glosario .....	12
1.1. Introducción .....	13
1.2. Sistema de nombre de dominio .....	13
1.2.1. Resolución .....	14
1.2.2. Nombre de dominio .....	14
1.2.3. Objetivos .....	14
1.2.4. Niveles de dominio .....	15
1.3. Zonas de búsquedas, tipos de servidores DNS y registros .....	15
1.3.1. Tipos de servidores DNS .....	17
1.3.2. Registros DNS .....	17
1.4. Funcionamiento del servicio DNS y tipos de consultas .....	18
1.4.1. Consulta recursiva .....	20
1.4.2. Consulta iterativa .....	21
1.4.3. Consulta inversa .....	21
1.5. Instalación y configuración de un servidor DNS en SO Linux .....	21
1.6. Servicio de directorio: características y funcionalidad .....	29
1.7. Organización de LDAP .....	29
1.8. Archivos básicos de configuración y uso .....	31
1.9. Instalación de OpenLDAP en SO Linux .....	33
1.10. Adaptación de la configuración del servidor de directorios para el despliegue de la aplicación. Usuarios centralizados .....	37
1.10.1. Autenticación en el servicio de directorio .....	37
1.10.2. Usuarios centralizados .....	39

Resumen .....	43
Supuestos prácticos .....	43
Ejercicios propuestos .....	44
Actividades de autoevaluación .....	44
<b>2. INSTALACIÓN Y ADMINISTRACIÓN DE SERVIDORES DE TRANSFERENCIA DE ARCHIVOS .....</b>	<b>47</b>
Objetivos .....	47
Mapa conceptual .....	48
Glosario .....	48
2.1. Introducción .....	49
2.2. Servicio de transferencia de archivos. Permisos y cuotas .....	49
2.2.1. Permisos .....	50
2.2.2. Cuotas .....	53
2.3. Tipos de usuarios, accesos al servicio y transferencia de ficheros .....	57
2.3.1. Tipos de usuarios .....	57
2.3.2. Tipos de accesos al servicio .....	57
2.3.3. Tipos de transferencia de ficheros .....	58
2.4. Modos de conexión al cliente .....	59
2.4.1. Modo activo .....	59
2.4.2. Modo pasivo .....	59
2.5. Protocolo seguro de transferencia de archivos .....	59
2.6. Utilización de herramientas gráficas y en modo texto. Comandos .....	61
2.6.1. Herramientas .....	61
2.6.2. Comandos .....	63
2.7. Instalación y configuración del servidor proFTPd en SO Linux .....	64
2.7.1. Validación mediante un host virtual .....	67
2.7.2. Validación del servicio FTP mediante LDAP .....	68
2.8. Utilización del servicio de transferencia de archivos .....	71
2.8.1. Desde el navegador .....	71
2.8.2. En el proceso de despliegue de la aplicación web .....	72
Resumen .....	73
Supuestos prácticos .....	73
Ejercicios propuestos .....	74
Actividades de autoevaluación .....	74
<b>3. IMPLANTACIÓN DE ARQUITECTURAS WEB .....</b>	<b>77</b>
Objetivos .....	77
Mapa conceptual .....	78
Glosario .....	78
3.1. Introducción .....	79
3.2. Arquitecturas web .....	79
3.3. Evolución de la tecnología web .....	80
3.4. Tecnologías usadas en aplicaciones web .....	81
3.4.1. En el lado servidor .....	81
3.4.2. En el lado cliente .....	82
3.4.3. En ambos .....	82
3.5. Servidores y aplicaciones libres y propietarias .....	83
3.6. Protocolo HTTP vs HTTPS .....	85

<b>3.7. Clasificación de servidores de aplicaciones del mercado actual .....</b>	86
<b>3.8. Instalación y configuración básica del servidor Apache .....</b>	87
3.8.1. Definición y características .....	87
3.8.2. Instalación y configuración del servidor Apache en Debian .....	88
3.8.3. Instalación y configuración del servidor IIS en Windows Server .....	94
<b>3.9. Estructura y recursos que componen una aplicación web. Descriptor de despliegue .....</b>	98
3.9.1. Archivos war .....	99
3.9.2. Descriptor de despliegue .....	100
<b>Resumen .....</b>	101
<b>Supuestos prácticos .....</b>	101
<b>Ejercicios propuestos .....</b>	102
<b>Actividades de autoevaluación .....</b>	102
<b>4. ADMINISTRACIÓN DE SERVIDORES WEB .....</b>	105
<b>Objetivos .....</b>	105
<b>Mapa conceptual .....</b>	106
<b>Glosario .....</b>	106
<b>4.1. Introducción .....</b>	107
<b>4.2. Configuración avanzada del servidor web .....</b>	107
4.2.1. Directivas de control del servidor Apache .....	107
4.2.2. Parámetros del servidor .....	109
<b>4.3. Hosts virtuales. Creación, configuración y utilización .....</b>	110
4.3.1. Hosts virtuales basados en nombre .....	110
4.3.2. Hosts virtuales basados en IP .....	113
4.3.3. Host virtual mixto .....	116
<b>4.4. Módulos: instalación, configuración y uso .....</b>	116
<b>4.5. Autenticación y control de acceso a directorios .....</b>	119
4.5.1. Establecimiento del control de acceso .....	120
4.5.2. Autenticación básica .....	121
4.5.3. Autenticación de usuarios mediante LDAP .....	123
<b>4.6. Certificados. Servidores de certificados .....</b>	124
4.6.1. Módulo SSL para Apache .....	124
4.6.2. Servidor virtual seguro en Apache .....	125
<b>4.7. Pruebas de funcionamiento, monitorización y rendimiento del servidor web .....</b>	127
4.7.1. Registro y monitorización .....	127
4.7.2. Directivas para archivos de registro, log y error .....	129
4.7.3. Pruebas de rendimiento del servidor web .....	130
<b>4.8. Configuración de hosts virtuales en SO Windows .....</b>	131
<b>Resumen .....</b>	133
<b>Supuestos prácticos .....</b>	134
<b>Ejercicios propuestos .....</b>	134
<b>Actividades de autoevaluación .....</b>	135
<b>5. ADMINISTRACIÓN DE SERVIDORES DE APLICACIONES .....</b>	137
<b>Objetivos .....</b>	137
<b>Mapa conceptual .....</b>	138
<b>Glosario .....</b>	138
<b>5.1. Introducción .....</b>	139

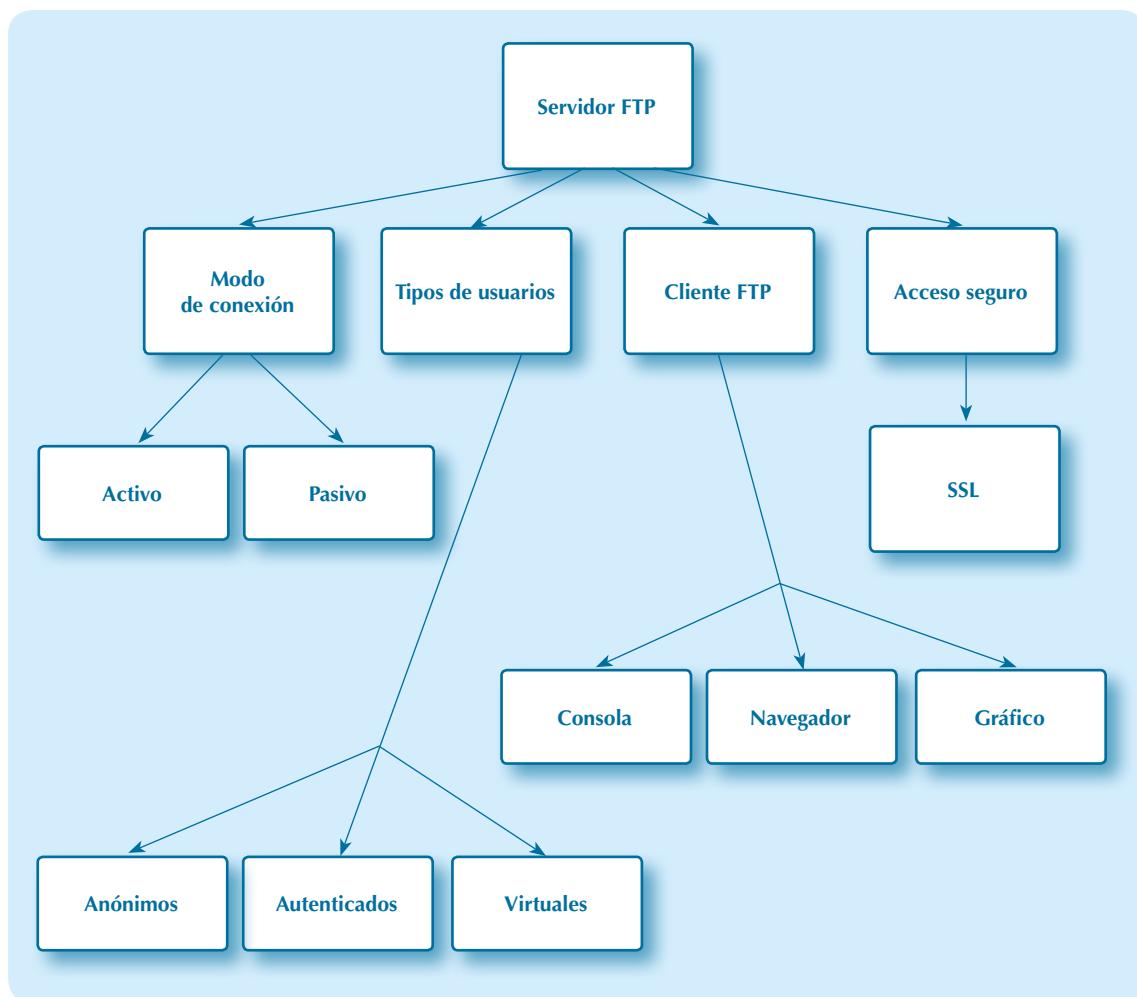
<b>5.2. Arquitectura y configuración básica del servidor de aplicaciones .....</b>	139
5.2.1. Instalación del servidor de aplicaciones Apache-Tomcat .....	140
5.2.2. Arquitectura de Apache-Tomcat y variables de entorno .....	145
<b>5.3. Administrar aplicaciones web .....</b>	149
<b>5.4. Autenticación de usuarios. Dominios de seguridad para la autenticación .....</b>	153
<b>5.5. Administración de sesiones. Sesiones persistentes .....</b>	159
<b>5.6. Archivos de registro de acceso y filtro de solicitudes .....</b>	161
<b>5.7. Instalación y configuración del servidor de aplicaciones en SO Windows .....</b>	168
<b>5.8. Despliegue de aplicaciones en el servidor de aplicaciones .....</b>	169
<b>5.9. Seguridad en el servidor de aplicaciones. Configurar el servidor de aplicaciones con soporte SSL/T .....</b>	174
5.9.1. Seguridad y autenticación .....	174
5.9.2. Configuración SSL sobre Tomcat .....	175
<b>Resumen .....</b>	177
<b>Supuestos prácticos .....</b>	178
<b>Ejercicios propuestos .....</b>	179
<b>Actividades de autoevaluación .....</b>	180
<b>6. DOCUMENTACIÓN Y SISTEMAS DE CONTROL DE VERSIONES .....</b>	183
<b>Objetivos .....</b>	183
<b>Mapa conceptual .....</b>	184
<b>Glosario .....</b>	184
<b>6.1. Introducción .....</b>	185
<b>6.2. Herramientas externas para la generación de documentación. Instalación, configuración y uso .....</b>	185
6.2.1. Instalación, configuración y uso de Javadoc .....	186
6.2.2. Instalación, configuración y uso de phpDocumentor .....	188
6.2.3. Instalación, configuración y uso de Doxygen .....	192
<b>6.3. Formatos estándar para la documentación .....</b>	194
<b>6.4. Creación y utilización de plantillas .....</b>	197
<b>6.5. Herramientas colaborativas para la elaboración y mantenimiento de la documentación .....</b>	200
6.5.1. Herramienta Slack .....	200
6.5.2. Herramienta Microsoft Office 365 .....	203
<b>6.6. Instalación, configuración y uso de sistemas de control de versiones en SO Windows .....</b>	204
6.6.1. Conceptos básicos .....	205
6.6.2. Funcionamiento del control de versiones .....	205
6.6.3. Instalación y configuración de Git en Netbeans .....	207
<b>6.7 Operaciones avanzadas .....</b>	211
<b>6.8. Seguridad de los sistemas de control de versiones .....</b>	214
6.8.1. Protocolo SSH .....	214
6.8.2. Protocolo HTTPS .....	215
<b>6.9. Historia de un repositorio .....</b>	215
<b>Resumen .....</b>	216
<b>Supuestos prácticos .....</b>	217
<b>Ejercicios propuestos .....</b>	218
<b>Actividades de autoevaluación .....</b>	218

# Instalación y administración de servidores de transferencia de archivos

## Objetivos

- ✓ Instalar y configurar servidores de transferencia de archivos.
- ✓ Crear usuarios y grupos para el acceso remoto al servidor.
- ✓ Configurar el acceso anónimo.
- ✓ Comprobar el acceso al servidor, tanto en modo activo como en modo pasivo.
- ✓ Usar el protocolo seguro de transferencia de archivos.
- ✓ Configurar y utilizar servicios de transferencia de archivos integrados en servidores web.
- ✓ Emplear el navegador como cliente del servicio de transferencia de archivos.

## Mapa conceptual



### Glosario

**Cortafuegos.** Es un componente software o hardware que permite bloquear el acceso no autorizado y permitir las comunicaciones deseadas en nuestra organización.

**FTP.** Es el protocolo de aplicación de transferencia de ficheros que intercambia información entre dos dispositivos conectados a una red TCP.

**Internet.** Es una red de redes que permite la interconexión de dispositivos mediante el conjunto de protocolos TCP/IP.

**Paquetes Linux.** Son programas que se pueden instalar mediante el comando apt-get en las distribuciones Linux y que forman parte del repositorio que posea cada distribución.

**Puerto de conexión UDP o TCP.** Es un número que va desde el 0 hasta el 65535 y sirve para enviar y recibir datos mediante el socket.

**Socket.** Es un ente abstracto a bajo nivel que permite la comunicación y el intercambio de datos entre un cliente y un servidor. Los sockets se pueden programar. Un socket se identifica mediante una IP y un puerto.

**TCP.** Es el protocolo orientado a conexión dentro del modelo TCP/IP que se encarga de crear las conexiones entre dos dispositivos mediante puertos. Es fundamental dentro del funcionamiento de Internet.

**UDP.** Es el protocolo no orientado a conexión en redes IP y a nivel de transporte. Se encarga de la trasmisión de información sin conexión de datagramas y mediante puertos.

## 2.1. Introducción

El servicio de transferencia de ficheros tiene un papel fundamental a la hora de desplegar una aplicación. Su función es transferir la información de desarrollo a producción en un entorno empresarial.

En el mundo tecnológico existen distintos servidores FTP. Para poder trabajar con ellos, se ha elegido la instalación y configuración de proFTPD, por ser uno de los más completos.

Existen varios modos de conexión, como son el activo y el pasivo, que van a depender de si existe un cortafuegos en mitad de la conexión o no.

Por otro lado, existen tres tipos de usuarios que se pueden habilitar en este tipo de servicio, como son usuarios autenticados, virtuales y anónimos.

## 2.2. Servicio de transferencia de archivos. Permisos y cuotas

Es un protocolo de red TCP que permite la transferencia de archivos entre sistemas conectados entre sí. Se basa en la arquitectura cliente-servidor del RFC 959. De manera que desde un cliente existe la posibilidad de conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos, independientemente del sistema operativo. El sistema operativo instalado y configurado en cada equipo es multiplataforma y heterogéneo.

La transferencia de archivos puede ser de todo tipo, como imágenes, vídeos, texto, etc., entre el cliente y el servidor. El interfaz de transferencia puede ser mediante comandos o modo gráfico. Aunque es uno de los métodos más usados en Internet, tiene un gran inconveniente, que es la seguridad, si no se configura correctamente y se toman las medidas oportunas para evitar el acceso fraudulento de la información que se transfiere.

Como se ha comentado anteriormente, este servicio se basa en una arquitectura cliente-servidor, siendo el cliente quien solicita la conexión para transferir los archivos y el servidor es el que ofrece o almacena archivos dependiendo de la solicitud del cliente. Por lo tanto, es

un servicio orientado a conexión que necesita establecer una conexión para poder transferir archivos.

Es necesario usar este servicio acompañado de algún protocolo de seguridad, como puede ser SSL, ya que de no hacerlo se corre el riesgo de que la información transferida sea hackeada por entidades externas.

El servidor de FTP funciona a través de los siguientes puertos configurables:

- Puerto 21: control de la conexión.
- Puerto 20 o mayor de 2014: puerto de transferencia de datos.

Hay que tener en cuenta que estos puertos son modificables mediante los archivos de configuración correspondientes. Pero si no se configura nada, por defecto, los puertos anteriores son utilizados por la arquitectura.

### 2.2.1. Permisos

Los permisos y las cuotas son una parte importante de la configuración del servicio FTP. Es necesario controlar el espacio y los permisos de lectura y escritura a usuarios que entran en el sistema desde el exterior. De no hacerlo así, podría aumentar el riesgo de amenaza desde el exterior y convertirse en riesgo real. Las amenazas podrían ser desde entrar en otro directorio que no sea el dedicado para el FTP, hasta que se caiga el sistema por falta de espacio.

Antes de entrar en detalle con las cuotas, se va a proceder a detallar cómo funcionan los permisos en Linux, para posteriormente explicar cómo a un usuario se le asignan los permisos.

Cuando se crea un fichero o carpeta en Linux, existen tres niveles de acceso que permiten controlar sus accesos, que son los siguientes:

- a) *Nivel propietario*: son los permisos que se asignan al propietario del archivo o directorio.
- b) *Nivel grupo*: son aquellos que se asignan a los grupos de usuarios. Esto es, un grupo puede tener de 1 a n usuarios.
- c) *Nivel usuarios*: este nivel corresponde a todos los usuarios definidos en el sistema operativo que no son los anteriores, o llamados “los otros”.



#### TOMA NOTA

El servicio de FTP trabaja con puertos: 21 de control y 20 de transferencia de datos.

Los permisos en Linux son tres y se distinguen de la siguiente forma:

1. *Lectura (r)*: el usuario podrá ver el contenido y visualizar un fichero o directorio. Si tiene asignado (-) no podrá visualizarlo.
2. *Escritura (w)*: el usuario podrá modificar el contenido del archivo o directorio.
3. *Ejecución (x)*: el usuario podrá ejecutar el archivo.

Normalmente son aplicados estos permisos para archivos ejecutables.

Y se le pueden aplicar a cada uno de los niveles anteriores. Por ejemplo, cuando nosotros creamos un archivo o directorio con el usuario root, y listamos el directorio con el comando ls -l, saldría algo parecido a la pantalla de la figura 2.1.

```
root@osboxes:~# ls -l
total 40
drwxr-xr-x 2 root root 4096 mar 16 12:53 Desktop
drwxr-xr-x 2 root root 4096 nov 23 2017 Documents
drwxr-xr-x 2 root root 4096 nov 23 2017 Downloads
drwxr-xr-x 2 root root 4096 nov 23 2017 Music
drwxr-xr-x 2 root root 4096 mar 29 14:17 Pictures
drwxr-xr-x 2 root root 4096 abr 3 05:11 prueba
-rw-r--r-- 1 root root 20 mar 29 15:36 prueba.txt
drwxr-xr-x 2 root root 4096 nov 23 2017 Public
drwxr-xr-x 2 root root 4096 nov 23 2017 Templates
drwxr-xr-x 2 root root 4096 nov 23 2017 Videos
```

**Figura 2.1**  
Listado de ficheros



#### PARA SABER MÁS

El comando ls -l permite conocer los permisos que tiene cada fichero o directorio. Investiga y prueba todas las opciones que permite el comando ls.

Se va a explicar cada una de las partes que acompañan a cada fichero o directorio:

- El primer carácter identifica a los siguientes tipos de ficheros:
  - (d): es un directorio.
  - (-): es un fichero.
  - (l): representa un enlace (link).
  - (b): indica que es un archivo binario.
  - (p): es un archivo especial de cauce (tubería).
  - (c): es un archivo de caracteres especiales, como puede ser una impresora.
- Después del primer carácter le siguen rwxr-xr-x, que son los permisos correspondientes al propietario del directorio o archivo en sus primeros tres caracteres, los tres siguientes son los correspondientes al grupo y los últimos tres caracteres están relacionados con los demás usuarios del sistema operativo.
- Después de los caracteres anteriores, aparece un número que indica el número de enlaces al archivo.
  - El primer root corresponde al usuario propietario del archivo o directorio.
  - El segundo root corresponde al grupo al que pertenece el archivo.
  - Las siguientes columnas representan el tamaño, fecha y hora de la última modificación del archivo o directorio.
  - La última columna es el nombre del directorio o archivo.

## Actividad propuesta 2.1



Explica cada uno de los campos que acompañan al directorio o fichero del sistema operativo.

Para asignar permisos en Linux se usan los siguientes comandos:

1. *chmod*: este comando puede modificar el permiso del propietario (u), los grupos (g) y los otros (o). Existen multitud de opciones para usar este comando, incluso se puede usar el sistema octal para aplicar permisos. La sintaxis general del comando es la siguiente:

```
chmod [opciones] modo-octal fichero.
```

El modo octal relacionado con los permisos aplicados a las tres columnas sería el siguiente:

Número decimal	Binario	Permisos efectivos
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwx

Por ejemplo, si se quiere asignar permisos de lectura (r) y escritura (w) al fichero prueba.txt al usuario propietario solo sería de la forma:

```
chmod 600 prueba.txt o  
chmod u+rw prueba.txt
```

2. *chown*: permite cambiar el propietario del archivo o directorio. La estructura general del comando sería la siguiente:

```
chown [opciones] [usuario] [:grupo] ficheros
```

Por ejemplo, si se quiere hacer propietario a Javier del fichero prueba.txt sería de la siguiente forma:

```
chown javier prueba.txt
```



## Actividad propuesta 2.2

Crea un fichero de texto y le das permiso de lectura y escritura al propietario, grupo y otros.

### 2.2.2. Cuotas

A continuación, se va a demostrar cómo funcionan las cuotas, y para ello se instalará el servicio *quota* en el sistema operativo, además de realizar algunas configuraciones para que funcione el programa:

1. Instalación del programa *quota*, como se observa en la figura 2.2.

```
root@osboxes:~# apt-get install quota
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libtirpc-common libtirpc3
Paquetes sugeridos:
  libnet-ldap-perl rpcbind
Se instalarán los siguientes paquetes NUEVOS:
  libtirpc-common libtirpc3 quota
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 1981 no actualizados.
```

**Figura 2.2**  
Instalación de *quota*

2. El siguiente paso es configurar el fichero */etc/fstab* con las opciones *usrquota* y *grpquota*. Se pueden aplicar a todo el sistema de ficheros, pero lo más recomendable es donde se ubican los usuarios, que es el directorio */home*. Se puede observar en los recuadros de la figura 2.3.

```
GNU nano 2.8.7                               Fichero: /etc/fstab

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system>      <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=51373f23-eec3-4d51-97ad-8ec04b57b53f /          ext4    errors=remount-ro 0      1
# /boot was on /dev/sda2 during installation
UUID=3adf58e1-1f88-4d7f-ae59-aeb2002d3bc /boot        ext4    defaults        0      2
# /home was on /dev/sda4 during installation
UUID=4a94062c-d003-4b6a-9038-9283dd21f88a /home        ext4    defaults,usrquota,grpquota 0
# swap was on /dev/sda3 during installation
UUID=3c19fc72-61ef-4836-96ae-8160de1b5acd none        swap    sw            0      0
/dev/sr0           /media/cdrom0 udf,iso9660 user,noauto 0
```

**Figura 2.3**  
Configuración  
de *fstab*

3. Para que se apliquen los cambios, se han de ejecutar los siguientes comandos. Y se observarán las figuras 2.4 y 2.5.

```
# mount -o remount /home
# mount
```

```
root@osboxes:~# mount -o remount /home
root@osboxes:~# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=1010156k,nr_inodes=252539,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=205208k,mode=755)
/dev/sdal on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
```

**Figura 2.4**  
Comando mount

```
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=28,pgrp=1,timeout=0,minproto=5,direct,pipe_ino=9755)
mqqueue on /dev/mqueue type mqqueue (rw,nosuid,nodev,noexec,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
/dev/sda2 on /boot type ext4 (rw,relatime,data=ordered)
/dev/sda4 on /home type ext4 (rw,relatime,quota,usrquota,grpquota,data=ordered)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
```

**Figura 2.5**  
Comando mount

### Actividad propuesta 2.3



Prueba todas las opciones del comando *mount*, incluso ejecuta el comando *mount* en tu equipo y comprobarás qué directorios tienes montados.

4. A continuación, el sistema está preparado y, más concretamente, el directorio/home está preparado para soportar cuotas. Es necesario verificar que todo es correcto mediante el comando siguiente y se observará figura 2.6.

```
# quotacheck -augmv
```

```
root@osboxes:/home# quotacheck -ugmv /home
quotacheck: Your kernel probably supports journaled quota but
no journaled quota to avoid running quotacheck after an unclean
quotacheck: Quota for users is enabled on mountpoint /home
Please turn quotas off or use -f to force checking.
```

**Figura 2.6**  
Comando quotacheck

5. En la figura anterior se observa que parece que da un error, pero realmente lo que está diciendo es que las cuotas están habilitadas y que si se necesita chequear es necesario desactivarlas. A continuación, se verá cómo se activan y desactivan las cuotas, con los siguientes comandos:

```
# quotaon -ugv /home
# quotaoff -ugv /home
```

6. Una vez activado el servicio de cuota con el comando quotaon, se está en disposición de crear cuota, por ejemplo, al directorio *examen* y usuario del mismo nombre que se encuentra dentro de home, para ello se hará de la siguiente forma:

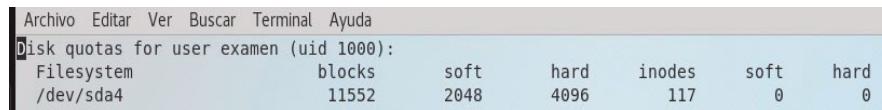
```
# setquota -u examen 2048 4096 0 0 /home
```

**CUADRO 2.1**  
**Opciones de setquota**

Comando	Descripción
examen	Usuario que se le aplica la cuota.
2048	Indica que el usuario examen tiene 2048 bloques de 1k para almacenar información.
4096	Si el usuario usa más de 4095 bloques de 1k obtendrá un mensaje de aviso que ha sobrepasado el límite. Y no podrá escribir más en el disco.
0	Indica que no hay límite para soft en los inodos.
0	Indica que no hay límite para hard en los inodos.
/home	Se aplica a la partición de home.

7. Después de haber asignado la cuota al usuario examen, se almacena en el directorio examen información para que sobrepase el límite colocado anteriormente. Y se ejecuta el comando siguiente:

```
# edquota -u examen
```



The screenshot shows a terminal window with the following text:

```
Archivo Editar Ver Buscar Terminal Ayuda
Disk quotas for user examen (uid 1000):
Filesystem      blocks    soft    hard   inodes    soft    hard
/dev/sda4        11552    2048    4096     117       0       0
```

**Figura 2.7**  
**Comando edquota**

Si lo hacemos por grupo, el comando sería el siguiente:

```
# edquota -g NombreGrupo
```

En la figura 2.7 aparecen conceptos nuevos que se explicarán en el siguiente cuadro:

**CUADRO 2.2**  
Opciones de edquota

Comando	Descripción
Filesystem	Ruta de montaje de /home.
Blocks	Indica que el número de bloques usados por el usuario en Kb.
Soft	Indicar el número de bloques en Kb antes de recibir un warning.
Hard	Indica el límite absoluto en Kb, que no podrá sobrepasar en ningún caso.
Inodes	Especifica el número de ficheros que puede usar el usuario.
Soft	Indica que no hay límite en el número de inodos.
Hard	Indica que no hay límite en el número de inodos.

8. El siguiente paso es listar la cuota del usuario en cuestión, o la de todos. Para ello se usarán los siguientes comandos y posteriormente se mostrará una imagen con su uso (figura 2.8).

```
# quota -u examen (muestra la cuota del usuario examen)
# repquota -a (muestra la cuota de todos los usuarios)
```

```
root@osboxes:/home# quota -u examen
Disk quotas for user examen (uid 1000):
  Filesystem blocks   quota   limit   grace   files   quota   limit   grace
    /dev/sda4   11552*   2048   4096   6days    117      0     0     0
root@osboxes:/home# repquota -a
*** Report for user quotas on device /dev/sda4
Block grace time: 7days; Inode grace time: 7days
                                Block limits          File limits
User        used   soft   hard grace   used   soft   hard grace
-----
root       --    32852     0     0      13      0     0     0
examen    +-   11552   2048   4096  6days    117      0     0
admin     --     24     0     0      6      0     0     0
#2000    --     12     0     0      3      0     0     0
```

**Figura 2.8**  
Comando vista cuota

**Actividad propuesta 2.4**



Crea un directorio dentro del sistema ficheros y le aplicas quota.

9. Por último, se puede establecer un tiempo de gracia (grace) que permite al usuario un tiempo para poder liberar espacio; por defecto en la instalación es de 6 días (el tiempo se ajusta en segundos). Se establecen 120 segundos para el usuario examen, como se observa en la figura 2.9.

```

root@osboxes:/home# setquota -u examen -T 120 unset /home
setquota: Not setting inode grace time on /dev/sda4 because softlimit is not exceeded.
root@osboxes:/home# repquota -a
*** Report for user quotas on device /dev/sda4
Block grace time: 7days; Inode grace time: 7days
      Block limits          File limits
User    used   soft   hard grace   used   soft   hard grace
-----
root     --  32852     0     0      13     0     0
examen   +- 11552  2048 4096 00:02   117     0     0
admin     --    24     0     0      6     0     0
#2000    --    12     0     0      3     0     0

```

**Figura 2.9**  
Opción Grace

## 2.3. Tipos de usuarios, accesos al servicio y transferencia de ficheros

### 2.3.1. Tipos de usuarios

Existen tres grandes grupos de usuarios que se pueden conectar al servidor para almacenar o recuperar información, que se comentan a continuación:

- Usuarios anónimos*: tienen acceso pero los permisos están limitados por el sistema de archivos. Para conectarse al sistema usan una cuenta simbólica como anonymous y como password una cuenta de correo electrónico. Este tipo de usuario es un agujero de seguridad, por lo que es necesario tomar las medidas oportunas para evitar posibles accesos no deseados a la información.
- Usuarios autenticados*: son aquellos que son propios del sistema operativo. Se requiere de un usuario y contraseña para entrar en el servidor FTP.
- Usuarios virtuales*: se crean independientemente del sistema operativo con sus directorios home apropiados y creados para tal fin. Servidores como proFTPD poseen este tipo de usuarios que permiten no comprometer la seguridad del sistema, ya que no están creados en el mismo. La validación de estos usuarios no tiene por qué realizarla el sistema, sino que puede ser en un fichero de texto, una base de datos como Mysql o un servicio de directorio como LDAP.

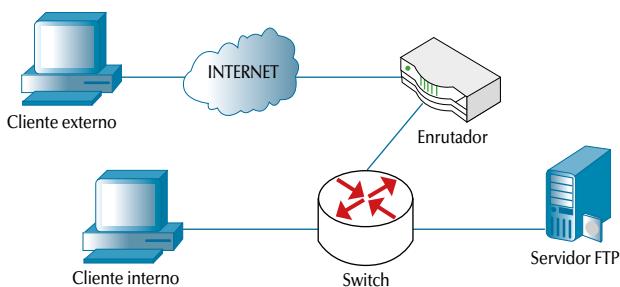


### Actividad propuesta 2.5

Comenta las diferencias entre los distintos tipos de usuarios que se pueden crear en el servicio FTP.

### 2.3.2. Tipos de accesos al servicio

Con relación al acceso al servicio de FTP, se puede acceder de diferentes formas, ya sea desde una red local o desde Internet. A continuación se pondrá un esquema de cómo acceder al servicio de FTP desde un cliente:



**Figura 2.10**  
Acceso al FTP

### 2.3.3. Tipos de transferencia de ficheros

A la hora de transferir archivos es necesario distinguir dos tipos de archivos para que la información que se traspase no sea inconsistente. Se comentan los tipos:

- ✓ *Archivos binarios*: son aquellos archivos que no son de texto y están codificados, por ejemplo, serían los archivos tipo ejecutable, imágenes, archivos de audio y vídeo, etc. El comando para poder cambiar al tipo de fichero es *binary*.
- ✓ *Archivos de texto*: son ficheros de tipo ASCII, legibles totalmente, esto es, se puede interpretar la información fácilmente. Se representa el fichero ASCII mediante 7 dígitos binarios en base decimal para representar la información. Un ejemplo de este tipo de ficheros son los que terminan en .txt, .xml, .html, .ps, etc. El comando para poder cambiar al tipo de fichero es el comando *ascii*.

#### Actividad propuesta 2.6



Define qué tipos de ficheros son: fichero Word, .html, archivo de sonido y archivo de vídeo.

Es crucial saber de antemano qué ficheros se van a transferir, ya que, si no se usan las opciones adecuadas, se podría destruir la información. El servicio FTP permite configurar las opciones adecuadas en la transferencia de ficheros.

En la figura 2.11 se demuestra cómo se usan las dos opciones anteriores en la línea de comandos de la consola del servicio FTP:

```
root@osboxes:/etc/proftpd# ftp localhost
Connected to localhost.
220 ProFTPD Server (Servidor FTP) [::1]
Name (localhost:root): admin
331 Contraseña necesaria para admin
Password:
230 Usuario admin conectado
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 Tipo establecido en I
ftp> ASCII
?Invalid command
ftp> ascii
200 Tipo establecido en A
ftp>
```

**Figura 2.11**  
Tipos de ficheros

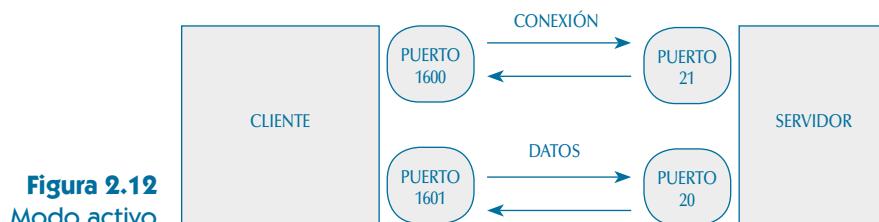
## 2.4. Modos de conexión al cliente

Cuando se realiza la comunicación entre el cliente y servidor existen dos modos de conexión por parte del cliente: modo activo y pasivo.

### 2.4.1. Modo activo

En el modo activo el servidor siempre crea un canal para datos por el puerto 20, mientras que el cliente asocia un puerto aleatorio mayor que 1024. El cliente envía un paquete al servidor, indicando el número de puerto para transferir archivos.

Se puede observar en la siguiente figura el modo activo en funcionamiento:

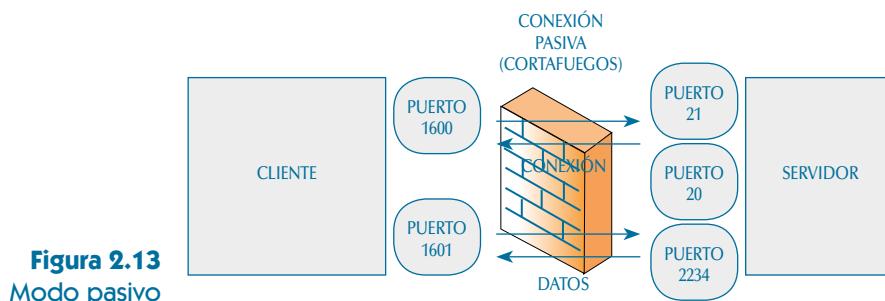


**Figura 2.12**  
Modo activo

### 2.4.2. Modo pasivo

Sin embargo, en modo pasivo, es el cliente quien comienza la conexión con el servidor para evitar bloqueos de conexión mediante configuraciones NAT o cortafuegos. En este modo, el cliente inicia ambas conexiones, control y datos. En este caso, si no existiera cortafuegos no habría ningún problema. Pero, al existir cortafuegos, el servidor, que intenta conectarse, devuelve la respuesta por un puerto diferente, que hace que el cortafuegos bloquee la conexión.

Con cortafuegos el diagrama de la conexión sería el siguiente:



**Figura 2.13**  
Modo pasivo

## 2.5. Protocolo seguro de transferencia de archivos

La instalación que se va a realizar es el servidor FTP en modo seguro con certificado y configurado en el fichero tls.conf para SO Linux bajo la versión de Debian y, más concretamente, de

Kali Linux. La instalación se puede realizar en una máquina virtual, que posee una imagen de este sistema operativo o en una máquina física. El procedimiento de instalación es el siguiente:

1. El primer paso es descomentar la línea que permite incluir el fichero `tls.conf` para configurar la conexión segura:

```
#include /etc/proftpd/tls.conf
```

2. Posteriormente, habría que eliminar el comentario en las siguientes líneas del fichero `tls.conf` para comprobar que funciona la seguridad en la conexión con el servidor FTP (figura 2.14).

```
<IfModule mod_tls.c>
TLSEngine on
TLSLog /var/log/proftpd/tls.log
SSLProtocol SSLv3
TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key
```

**Figura 2.14**  
Fichero `tls.conf`

3. El siguiente paso es generar las claves públicas que se colocarán en la ruta `/etc/ssl` mediante el comando `proftpd-gencert`, y obtenemos la pantalla de la figura 2.15.

```
root@osboxes:/etc/proftpd# proftpd-gencert
Generating a 2048 bit RSA private key
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/proftpd.key'
-----
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]:ES
State or Province Name (full name) [Some-State]:Cordoba
Locality Name (eg, city) []:Cordoba
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Educacion
Organizational Unit Name (eg, section) []:Practica
Common Name (e.g. server FQDN or YOUR name) []:FTP
Email Address []:

Use the following information in your ProFTPD configuration:
TLSRSACertificateFile /etc/ssl/certs/proftpd.crt
TLSRSACertificateKeyFile /etc/ssl/private/proftpd.key
```

**Figura 2.15**  
Fichero certificado

4. A continuación, se va a proceder a dar los permisos adecuados a los ficheros generados:

```
#chmod 600 /etc/ssl/private/proftpd.key
#chmod 644 /etc/ssl/certs/proftpd.crt
```

5. Por último, reiniciamos el servidor FTP con el comando siguiente. Y obtendremos la conexión segura con certificado, como se puede observar en la pantalla de la figura 2.16.

```
#service proftpd restart
```