

Servicio transferencia de archivos

Enjaulamiento
de usuarios

Índice

Servidor multisitio por puerto y enjaular usuario Ubuntu Server.....	3
Estado inicial.....	3
Configuración de sitios.....	5
Configuración de puertos para apache2.....	7
Comprobación de éxito de la apertura.....	9
Enjaular usuario.....	10
Editar /etc/ssh/sshd_config.....	11

Servidor multisitio por puerto y enjaular usuario Ubuntu Server.

Estado inicial.

El servidor Ubuntu es un clon del que se ha documentado en el Tema2 (configuración entorno de desarrollo y usuario).

Con el comando `hostnamectl` muestro versión de la distribución Linux de esta máquina.

```
miadmin@RST-USED:~$ hostnamectl
Static hostname: RST-USED
Icon name: computer-vm
Chassis: vm
Machine ID: e9e8456308cb444bb9b40f3a2e89e9ff
Boot ID: e0a343a68ca241618c7531dac325bcb8
Virtualization: oracle
Operating System: Ubuntu 22.04.1 LTS
Kernel: Linux 5.15.0-52-generic
Architecture: x86-64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
```

Compruebo primero los usuarios presentes en el servidor.

```
miadmin@RST-USED:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104:./nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1:./var/cache/pollinate:/bin/false
sshd:x:106:65534:./run/sshd:/usr/sbin/nologin
syslog:x:107:113:./home/syslog:/usr/sbin/nologin
uidd:x:108:114:./run/uidd:/usr/sbin/nologin
tcpdump:x:109:115:./nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117:./var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
miadmin:x:1000:1000:rstuslimpia:/home/miadmin:/bin/bash
lxd:x:999:100:./var/snap/lxd/common/lxd:/bin/false
operadorweb:x:1001:33:./var/www/html:/bin/sh
miadmin@RST-USED:~$
```

Puedo ver que están operadorweb y miadmin, dos usuarios creados en instalaciones anteriores, pero no hay ni rastro de daw201, que es el usuario que voy a crear y enjaular.

Para ello ejecuto el siguiente comando (`sudo useradd -m -d /var/www/puerto81 -g www-data daw201`). En el añado el usuario, dándole un home en /var/www/puerto81 y haciéndolo pertenecer al grupo www-data.

```
miadmin@RST-USED:~$ sudo useradd -m -d /var/www/puerto81 -g www-data daw201
miadmin@RST-USED:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uidd:x:108:114::/run/uidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
miadmin:x:1000:1000:rstuslimpia:/home/miadmin:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
operadorweb:x:1001:33::/var/www/html:/bin/sh
daw201:x:1002:33::/var/www/puerto81:/bin/sh
```

Aquí podemos ver al usuario nuevo y sus principales datos

Lo siguiente es crear en su home el directorio del que colgarán los proyectos subidos por él.

Y listar /var/www para comprobar si se ha creado correctamente.

```
miadmin@RST-USED:~$ sudo mkdir /var/www/puerto81/public_html
miadmin@RST-USED:~$ ls -l /var/www
total 8
drwxrwsr-x 8 operadorweb www-data 4096 oct 24 17:42 html
drwxr-x--- 3 daw201 www-data 4096 dic 14 17:31 puerto81
```

También le dotaremos de un password.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo passwd daw201
[sudo] password for miadmin:
New password:
Retype new password:
passwd: password updated successfully
```

Configuración de sitios.

Por seguridad, el primer paso será copiar la configuración inicial del archivo `/etc/apache2/sites-available/000-default.conf`, este paso es sumamente importante pues las modificaciones las haremos en el archivo modificado, dejando intacto el original.

Para ello primero hay que situarse en el directorio donde está este archivo.

```
miadmin@RST-USED:~$ cd /etc/apache2/sites-available
miadmin@RST-USED:/etc/apache2/sites-available$
```

Comprobamos que efectivamente se encuentra allí.

```
miadmin@RST-USED:/etc/apache2/sites-available$ ls -a
.  ..  000-default.conf  default-ssl.conf
```

Y ahora si, lo copiamos y lo volvemos a listar para ver que está copiado.

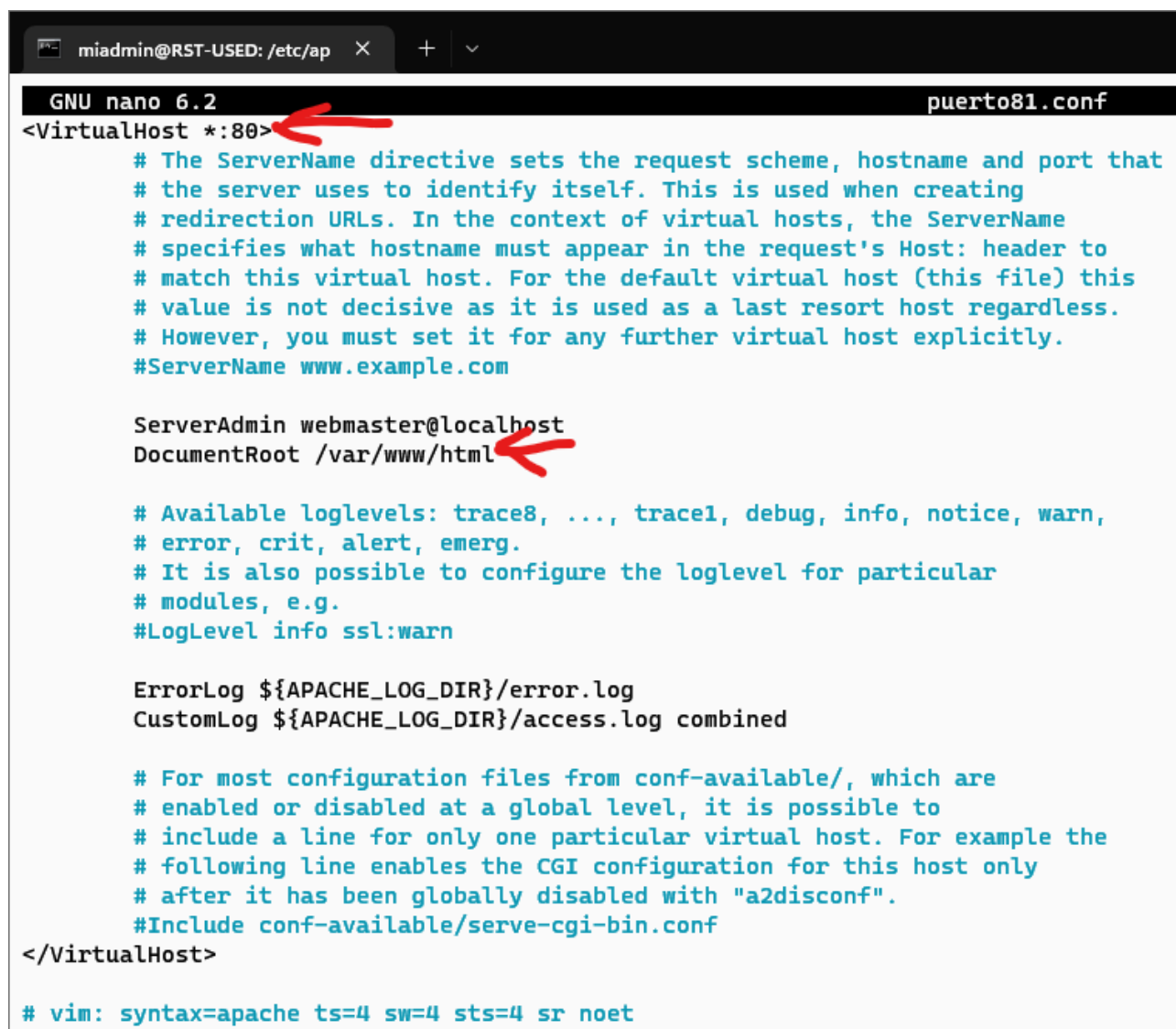
```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo cp 000-default.conf puerto81.conf
miadmin@RST-USED:/etc/apache2/sites-available$ ls -a
.  ..  000-default.conf  default-ssl.conf  puerto81.conf
```

Ahora es el turno de editar el fichero, cambiando el puerto de escucha (por defecto el 80) al 81 y documento raíz al directorio `public_html` que creamos en el home del nuevo usuario.

Comando para editar el fichero.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo nano puerto81.conf
```

Estado inicial del fichero.



```
miadmin@RST-USED: /etc/ap × + v
GNU nano 6.2 puerto81.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

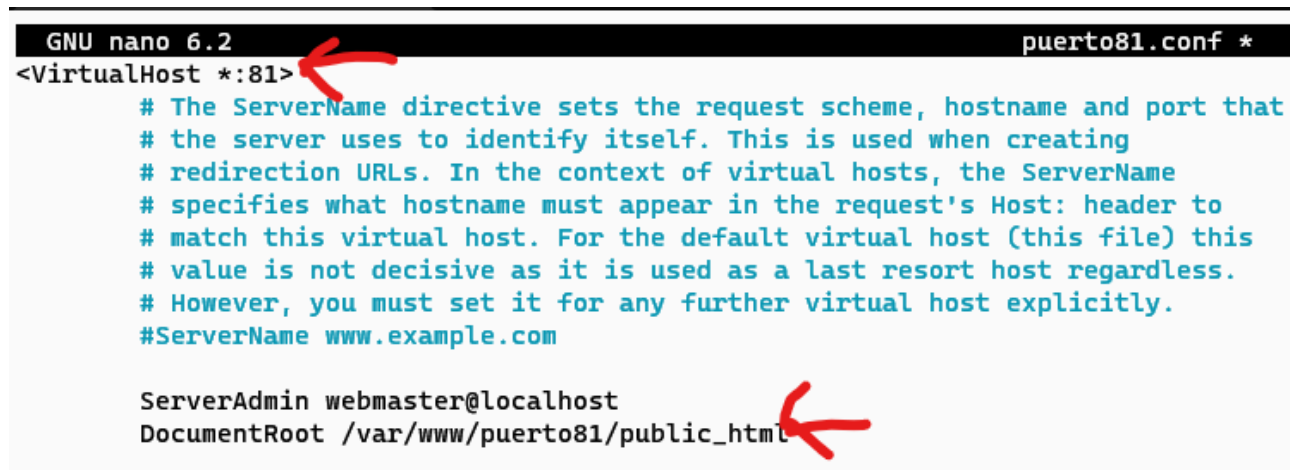
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Fichero después de modificarlo. No hay que modificar nada más que lo señalado por las flechas.



```
GNU nano 6.2 puerto81.conf *
<VirtualHost *:81>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/puerto81/public_html
```

Configuración de puertos para apache2.

Hay que modificar el fichero /etc/apache2/ports.conf, en él hay que incluir la siguiente línea

Listen 81

Estado original.

```
GNU nano 6.2 /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Estado después de la modificación.

```
GNU nano 6.2 /etc/apache2/ports.conf *
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80
Listen 81
<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Activación puerto 81.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo a2ensite puerto81
Enabling site puerto81.
To activate the new configuration, you need to run:
systemctl reload apache2
```

Y haciendo caso parcial a lo que nos dice la línea de comandos, hacemos un restart del servicio apache2 (en lugar del sugerido reload).

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo service apache2 restart
miadmin@RST-USED:/etc/apache2/sites-available$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-12-14 17:57:30 UTC; 6s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1930 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 1934 (apache2)
    Tasks: 6 (Limit: 2238)
   Memory: 10.1M
      CPU: 20ms
   CGroup: /system.slice/apache2.service
           └─1934 /usr/sbin/apache2 -k start
             └─1935 /usr/sbin/apache2 -k start
               └─1936 /usr/sbin/apache2 -k start
                 └─1937 /usr/sbin/apache2 -k start
                   └─1938 /usr/sbin/apache2 -k start
                     └─1939 /usr/sbin/apache2 -k start

dic 14 17:57:30 RST-USED systemd[1]: apache2.service: Deactivated successfully.
dic 14 17:57:30 RST-USED systemd[1]: Stopped The Apache HTTP Server.
dic 14 17:57:30 RST-USED systemd[1]: Starting The Apache HTTP Server...
dic 14 17:57:30 RST-USED apachectl[1933]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using
dic 14 17:57:30 RST-USED systemd[1]: Started The Apache HTTP Server.
Lines 1-22/22 (END)
```

Comprobamos como están en este punto de la instalación los puertos del servidor.

Aún no aparece el puerto 81.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo ufw status
Status: active
```

To	Action	From
22/tcp	ALLOW	Anywhere
80	ALLOW	Anywhere
9003	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)
80 (v6)	ALLOW	Anywhere (v6)
9003 (v6)	ALLOW	Anywhere (v6)

Así que lo ‘abrimos’.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo ufw allow 81
Rule added
Rule added (v6)
```

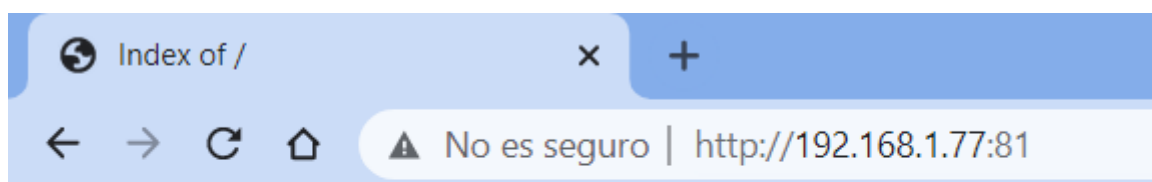

Y comprobamos de nuevo el estado de los puertos.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
80 ALLOW Anywhere
9003 ALLOW Anywhere
81 ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
80 (v6) ALLOW Anywhere (v6)
9003 (v6) ALLOW Anywhere (v6)
81 (v6) ALLOW Anywhere (v6)
```

Comprobación de éxito de la apertura.

Este es el índice por defecto que nos muestra el navegador si le pedimos por http que nos muestre lo que hay en nuestra dirección ip a través del puerto 81.



Index of /

[Name](#) [Last modified](#) [Size](#) [Description](#)

Apache/2.4.52 (Ubuntu) Server at 192.168.1.77 Port 81

Para personalizar este index, habremos de crear el nuestro propio y situarlo en la carpeta public_html para que sea a este nuevo index a donde nos redirija el navegador.

Es suficiente con un mensaje sencillo.

```
indexPuerto81.html > html
1  <!DOCTYPE html>
2  <html lang="en">
3  <head>
4      <meta charset="UTF-8">
5      <meta http-equiv="X-UA-Compatible" content="IE=edge">
6      <meta name="viewport" content="width=device-width, initial-scale=1.0">
7      <title>Index Puerto81</title>
8  </head>
9  <body>
10     <h1 style="color: red;">Hola desde el Puerto81</h1>
11 </body>
12 </html>
```

Y con la ayuda de Filezilla, lo vamos a situar en el directorio public_html, pero esto será después de enjaular al usuario daw201 y darle permisos.

Enjaular usuario.

Cambiamos el propietario del directorio home del usuario daw202 que es /var/www/puerto81 al usuario root y grupo root.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo chown root:root /var/www/puerto81
```

Comprobación.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo ls -l /var/www/puerto81
total 4
drwxr-xr-x 2 root root 4096 dic 14 17:31 public_html
```

Cambiaremos los permisos para que nadie pueda escribir (555).

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo chmod 555 /var/www/puerto81
miadmin@RST-USED:/etc/apache2/sites-available$
```

Cambiamos los permisos y propietario del directorio /var/www/puerto81/public_html al usuario daw202 y grupo www-data permisos para que el propietario como el grupo tenga permisos totales y el publico solo pueda ver y ejecutar con bit pegajoso y recursividad (2775).

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo chown -R daw201:www-data /var/www/puerto81/public_html/
miadmin@RST-USED:/etc/apache2/sites-available$
```

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo chmod -R 2775 /var/www/puerto81/public_html/  
miadmin@RST-USED:/etc/apache2/sites-available$
```

Creamos el grupo de usuarios enjaulados para simplificar la creacion de proximos usuarios.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo groupadd ftpusers
```

Añadimos el usuario al nuevo grupo.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo usermod -g ftpusers daw201
```

Y por último, comprobamos haberlo hecho correctamente.

```
miadmin@RST-USED:/etc/apache2/sites-available$ cat /etc/group | grep ftp  
ftpusers:x:1001:
```

```
miadmin@RST-USED:/etc/apache2/sites-available$ cat /etc/passwd | grep daw201  
daw201:x:1002:1001::/var/www/puerto81:/bin/sh
```

Editar /etc/ssh/sshd_config


Antes de editar lo mejor que podemos hacer es hacer una copia de seguridad del fichero anterior.

Para ello, nos desplazamos hasta su directorio y listamos.

```
miadmin@RST-USED:/etc/apache2/sites-available$ cd /etc/ssh  
miadmin@RST-USED:/etc/ssh$ ls -l  
total 548  
-rw-r--r-- 1 root root 505426 feb 25 2022 moduli  
-rw-r--r-- 1 root root 1650 feb 25 2022 ssh_config  
drwxr-xr-x 2 root root 4096 feb 25 2022 ssh_config.d  
-rw-r--r-- 1 root root 3281 sep 27 11:29 sshd_config  
drwxr-xr-x 2 root root 4096 feb 25 2022 sshd_config.d  
-rw----- 1 root root 1385 sep 27 11:29 ssh_host_dsa_key  
-rw-r--r-- 1 root root 606 sep 27 11:29 ssh_host_dsa_key.pub  
-rw----- 1 root root 513 sep 27 11:29 ssh_host_ecdsa_key  
-rw-r--r-- 1 root root 178 sep 27 11:29 ssh_host_ecdsa_key.pub  
-rw----- 1 root root 411 sep 27 11:29 ssh_host_ed25519_key  
-rw-r--r-- 1 root root 98 sep 27 11:29 ssh_host_ed25519_key.pub  
-rw----- 1 root root 2602 sep 27 11:29 ssh_host_rsa_key  
-rw-r--r-- 1 root root 570 sep 27 11:29 ssh_host_rsa_key.pub  
-rw-r--r-- 1 root root 342 dic 7 2020 ssh_import_id
```

Y a continuación, hacemos la copia y volvemos a listar para ver que se ha creado.


```
miadmin@RST-USED:/etc/ssh$ sudo cp sshd_config sshd_config.bak
miadmin@RST-USED:/etc/ssh$ ls -l
total 552
-rw-r--r-- 1 root root 505426 feb 25 2022 moduli
-rw-r--r-- 1 root root 1650 feb 25 2022 ssh_config
drwxr-xr-x 2 root root 4096 feb 25 2022 ssh_config.d
-rw-r--r-- 1 root root 3281 sep 27 11:29 sshd_config
-rw-r--r-- 1 root root 3281 dic 14 19:09 sshd_config.bak
drwxr-xr-x 2 root root 4096 feb 25 2022 sshd_config.d
-rw----- 1 root root 1385 sep 27 11:29 ssh_host_dsa_key
-rw-r--r-- 1 root root 606 sep 27 11:29 ssh_host_dsa_key.pub
-rw----- 1 root root 513 sep 27 11:29 ssh_host_ecdsa_key
-rw-r--r-- 1 root root 178 sep 27 11:29 ssh_host_ecdsa_key.pub
-rw----- 1 root root 411 sep 27 11:29 ssh_host_ed25519_key
-rw-r--r-- 1 root root 98 sep 27 11:29 ssh_host_ed25519_key.pub
-rw----- 1 root root 2602 sep 27 11:29 ssh_host_rsa_key
-rw-r--r-- 1 root root 570 sep 27 11:29 ssh_host_rsa_key.pub
-rw-r--r-- 1 root root 342 dic 7 2020 ssh_import_id
```



En el final del fichero sshd_config .

```
# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
PasswordAuthentication yes
```



```
^G Help      ^O Write Out  ^W Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```

Incluimos las siguientes sentencias.

Match Group ftpusers

ChrootDirectory %h

ForceCommand internal-sftp -u 2

AllowTcpForwarding yes

PermitTunnel no

X11Forwarding no

```
# override default of no subsystems
#Subsystem sftp /usr/lib/openssh/sftp-server
Subsystem sftp internal-sftp
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
PasswordAuthentication yes

Match Group ftpusers
ChrootDirectory %h
ForceCommand internal-sftp -u 2
AllowTcpForwarding yes
PermitTunnel no
X11Forwarding no
```

Comentamos esta línea

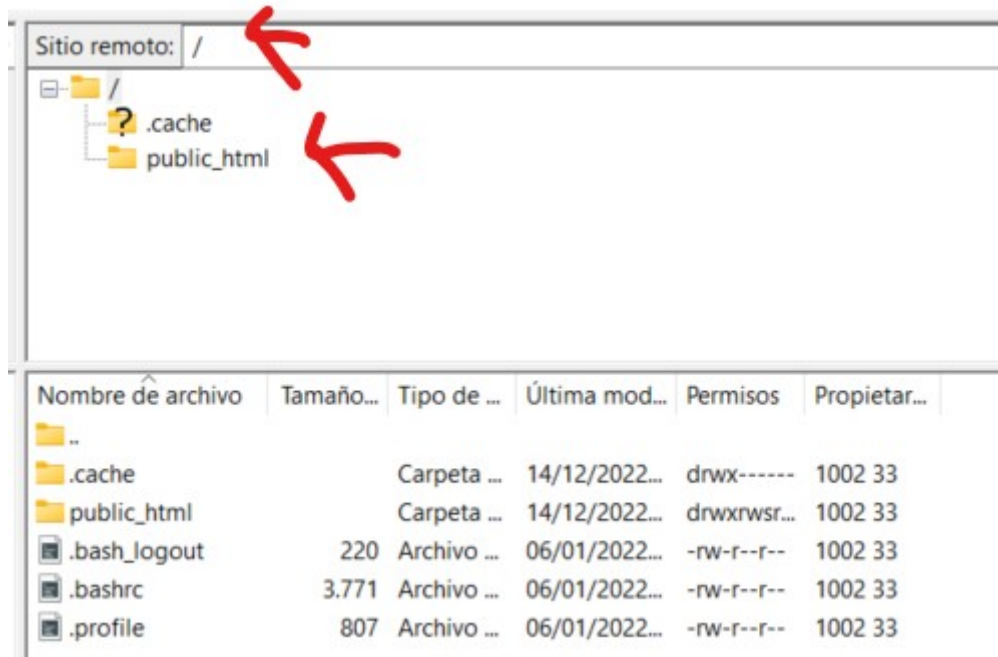
Añadimos esta.

Y añadimos estas líneas más. Ojo, respetar escrupulosamente.

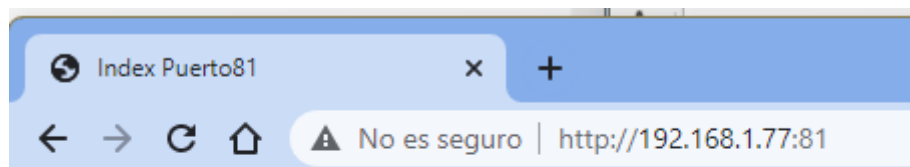
^G Help **^O** Write Out **^W** Where Is **^K** Cut
^X Exit **^R** Read File **^N** Replace **^U** Paste

Guardamos, salimos y reiniciamos el servidor para que todos los cambios se guarden.

Por último, usamos el Filezilla para subir el archivo index.html y comprobar que, como indican las flechas, nuestro usuario está correctamente enjaulado y su directorio raíz es también correcto.



Y ahora sí podemos escribir la ip del servidor y el puerto por el que escucha el directorio de este usuario y nos mostrará el index que hemos editado. **IMPORTANTE:** El archivo se ha de llamar index.html, el que aquí documenta lo llamó en primera instancia de otra manera y daba error. Subsanoado este, este es el resultado que demuestra que todo el trabajo está bien realizado.



Hola desde el Puerto81