

# CREACIÓN DE UN USUARIO Y SU ENJAULAMIENTO EN EL SERVIDOR

Manuel Martín Alonso

Lo primero que tenemos que hacer es crear el usuario mediante el comando **useradd**.

Crearemos el usuario **daw204** asignándole la carpeta home del usuario a **/var/www/puerto81** y asignándole el grupo **www-data**.

Cuando hayamos creado el usuario le asignaremos una contraseña mediante el comando **passwd** seguido del usuario al que queremos asignárselo.

```
miadmin@mma-used:~$ sudo useradd -m -d /var/www/puerto81 -g www-data daw204
[sudo] password for miadmin:
miadmin@mma-used:~$ cd /var/www
miadmin@mma-used:/var/www$ ls
html puerto81
miadmin@mma-used:/var/www$ sudo passwd daw204
New password:
Retype new password:
passwd: password updated successfully
miadmin@mma-used:/var/www$ _
```

Lo siguiente que tenemos que hacer es crear una carpeta llamada **public\_html** en la cual almacenaremos el index del usuario **daw204**.

```
miadmin@mma-used:/var/www$ sudo mkdir /var/www/puerto81/public_html
```

Para comprobar que la tenemos creada, pondremos **ls -l**.

```
miadmin@mma-used:/var/www$ ls -l
total 8
drwxrwsr-x 12 operadorweb www-data 4096 oct 24 20:21 html
drwxr-x---  3 daw204      www-data 4096 nov  5 19:03 puerto81
miadmin@mma-used:/var/www$
```

A continuación, copiaremos el archivo de la configuración inicial de apache y lo nombraremos **puerto81.conf**, y lo editaremos con **nano**.

```
miadmin@mma-used:/etc/apache2/sites-available$ sudo cp 000-default.conf puerto81.conf
```

Dentro del archivo cambiaremos el puerto por el que va a escuchar al **puerto 81** y cambiaremos la ruta donde tiene que ir a buscar el index, ubicado dentro de la carpeta **public\_html**.

```
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_

# 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
```

```
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

Lo siguiente que tenemos que hacer añadir dentro de los puertos de escucha de **apache2**, que escuche también por el **puerto 81**.

```
miadmin@mma-used:/etc/apache2$ ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars      mods-available  ports.conf    sites-enabled
miadmin@mma-used:/etc/apache2$ sudo nano ports.conf _
```

Para que escuche por el **puerto 81** deberemos añadir **Listen 81** debajo del **puerto 80**.

```
GNU nano 6.2                                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

[ Wrote 15 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^_ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

Para habilitar el nuevo sitio web utilizaremos el comando **a2ensite puerto81**. Además, deshabilitaremos el sitio web por defecto de apache con el comando **a2dissite**.

```
miadmin@mma-used:/etc/apache2$ sudo a2ensite puerto81
[sudo] password for miadmin:
Sorry, try again.
[sudo] password for miadmin:
Site puerto81 already enabled
```

```
miadmin@mma-used:/etc/apache2$ sudo a2dissite 000-default
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
miadmin@mma-used:/etc/apache2$ _
```

Una vez hecho todos los cambios, **reiniciaremos el servicio de apache y habilitaremos el puerto 81** mediante el comando **sudo ufw allow 81**.

```
miadmin@mma-used:/etc/apache2$ sudo service apache2 restart
miadmin@mma-used:/etc/apache2$ 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 Sat 2022-11-05 19:11:55 UTC; 10s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 1375 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1380 (apache2)
    Tasks: 6 (limit: 2238)
   Memory: 10.1M
      CPU: 59ms
   CGroup: /system.slice/apache2.service
           └─1380 /usr/sbin/apache2 -k start
             └─1381 /usr/sbin/apache2 -k start
               └─1382 /usr/sbin/apache2 -k start
                 └─1383 /usr/sbin/apache2 -k start
                   └─1384 /usr/sbin/apache2 -k start
                     └─1385 /usr/sbin/apache2 -k start

nov 05 19:11:55 mma-used systemd[1]: Starting The Apache HTTP Server...
nov 05 19:11:55 mma-used apachectl[1379]: AH00558: apache2: Could not reliably determine the server>
nov 05 19:11:55 mma-used systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

```
miadmin@mma-used:/etc/apache2$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
Apache ALLOW Anywhere
9003 ALLOW Anywhere
9000 DENY Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
Apache (v6) ALLOW Anywhere (v6)
9003 (v6) ALLOW Anywhere (v6)
9000 (v6) DENY Anywhere (v6)

miadmin@mma-used:/etc/apache2$
```

```
miadmin@mma-used:/etc/apache2$ sudo ufw allow 81
Rule added
Rule added (v6)
miadmin@mma-used:/etc/apache2$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
Apache ALLOW Anywhere
9003 ALLOW Anywhere
9000 DENY Anywhere
81 ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
Apache (v6) ALLOW Anywhere (v6)
9003 (v6) ALLOW Anywhere (v6)
9000 (v6) DENY Anywhere (v6)
81 (v6) ALLOW Anywhere (v6)

miadmin@mma-used:/etc/apache2$ _
```

Lo siguiente que tenemos que hacer es cambiar el propietario de la carpeta **puerto 80** y **puerto 81** para que pase a pertenecer al usuario **root** y al grupo **root**.

Cuando cambiemos los propietarios, cambiaremos los permisos tanto de la carpeta **puerto80** y de **puerto81**, teniendo los permisos de lectura y de ejecución.

Una vez hecho, le asignaremos el propietario a la carpeta **public\_html** asignándole como propietario al **daw204** y asignándole como grupo a **www-data**. Luego le aplicamos los permisos de lectura, escritura y ejecución a dicha carpeta, añadiéndole el sticky bit y mostraremos si se ha realizado correctamente mediante el comando **tree -gup /var/www**.

```
miadmin@mma-used:~$ sudo chown root:root /var/www/puerto80
[sudo] password for miadmin:
miadmin@mma-used:~$ sudo chown root:root /var/www/puerto81
miadmin@mma-used:~$ sudo chown root:root /var/www/puerto81
miadmin@mma-used:~$ sudo chmod 555 /var/www/puerto80
miadmin@mma-used:~$ sudo chmod 555 /var/www/puerto81
miadmin@mma-used:~$ ls -l
total 4
drwxrwxr-x 9 miadmin miadmin 4096 oct 20 09:48 apache-tomcat-9.0.68
miadmin@mma-used:~$ ls -l /var/www
total 12
drwxrwsr-x 11 operadorweb www-data 4096 oct 25 11:03 html
dr-xr-xr-x 4 root root 4096 oct 25 11:31 puerto80
dr-xr-xr-x 4 root root 4096 oct 25 11:31 puerto81
miadmin@mma-used:~$ sudo chown -R daw201:www-data /var/www/puerto80/public_html
miadmin@mma-used:~$ sudo chown -R daw202:www-data /var/www/puerto81/public_html
miadmin@mma-used:~$ sudo chmod -R 2775 /var/www/puerto80/public_html
miadmin@mma-used:~$ sudo chmod -R 2775 /var/www/puerto81/public_html
miadmin@mma-used:~$ _
```

```
[-rw-r--r-- operadorweb www-data] muestraEjercicio08.php
[-rw-r--r-- operadorweb www-data] muestraEjercicio09.php
[-rw-r--r-- operadorweb www-data] muestraEjercicio10.php
[-rw-r--r-- operadorweb www-data] muestraEjercicio12.php
[-rw-r--r-- operadorweb www-data] muestraEjercicio15.php
[-rw-r--r-- operadorweb www-data] muestraEjercicio16.php
[-rw-r--r-- operadorweb www-data] muestraEjercicio21.php
[-rw-r--r-- operadorweb www-data] muestraEjercicio22.php
[-rw-r--r-- operadorweb www-data] muestraEjercicio23.php
[drwxr-sr-x operadorweb www-data] tmp
[drwxr-sr-x operadorweb www-data] webroot
[drwxr-sr-x operadorweb www-data] css
[-rw-r--r-- operadorweb www-data] estilos.css
[-rw-r--r-- operadorweb www-data] curriculum-logo.png
[-rw-r--r-- operadorweb www-data] ejecutar.png
[-rw-r--r-- operadorweb www-data] favicon.ico
[-rw-r--r-- operadorweb www-data] github-logo.png
[-rw-r--r-- operadorweb www-data] imagenfondo.jpg
[-rw-r--r-- operadorweb www-data] logo_propio.png
[-rw-r--r-- operadorweb www-data] logo_propio-sinfondo.png
[-rw-r--r-- operadorweb www-data] mostrarcodigo.png
[-rw-r--r-- operadorweb www-data] portada-dwes.png
[-rw-r--r-- operadorweb www-data] volver.png
[drwxr-sr-x operadorweb www-data] webroot
[drwxr-sr-x operadorweb www-data] css
[-rw-r--r-- operadorweb www-data] estilos.css
[dr-xr-xr-x root root ] puerto80
[drwxrwsr-x daw201 www-data] public_html
[-rw-rwsr-x daw201 www-data] index.html
[dr-xr-xr-x root root ] puerto81
[drwxrwsr-x daw202 www-data] public_html
[-rw-rwsr-x daw202 www-data] index.html
30 directories, 120 files
miadmin@mma-used:~$ tree -gup /var/www_
```

Cuando hayamos hecho lo anterior, nos iremos a **/etc/ssh** y haremos una copia del archivo **sshd\_config** para editarlo con seguridad.

```
GNU nano 6.2 /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr>

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

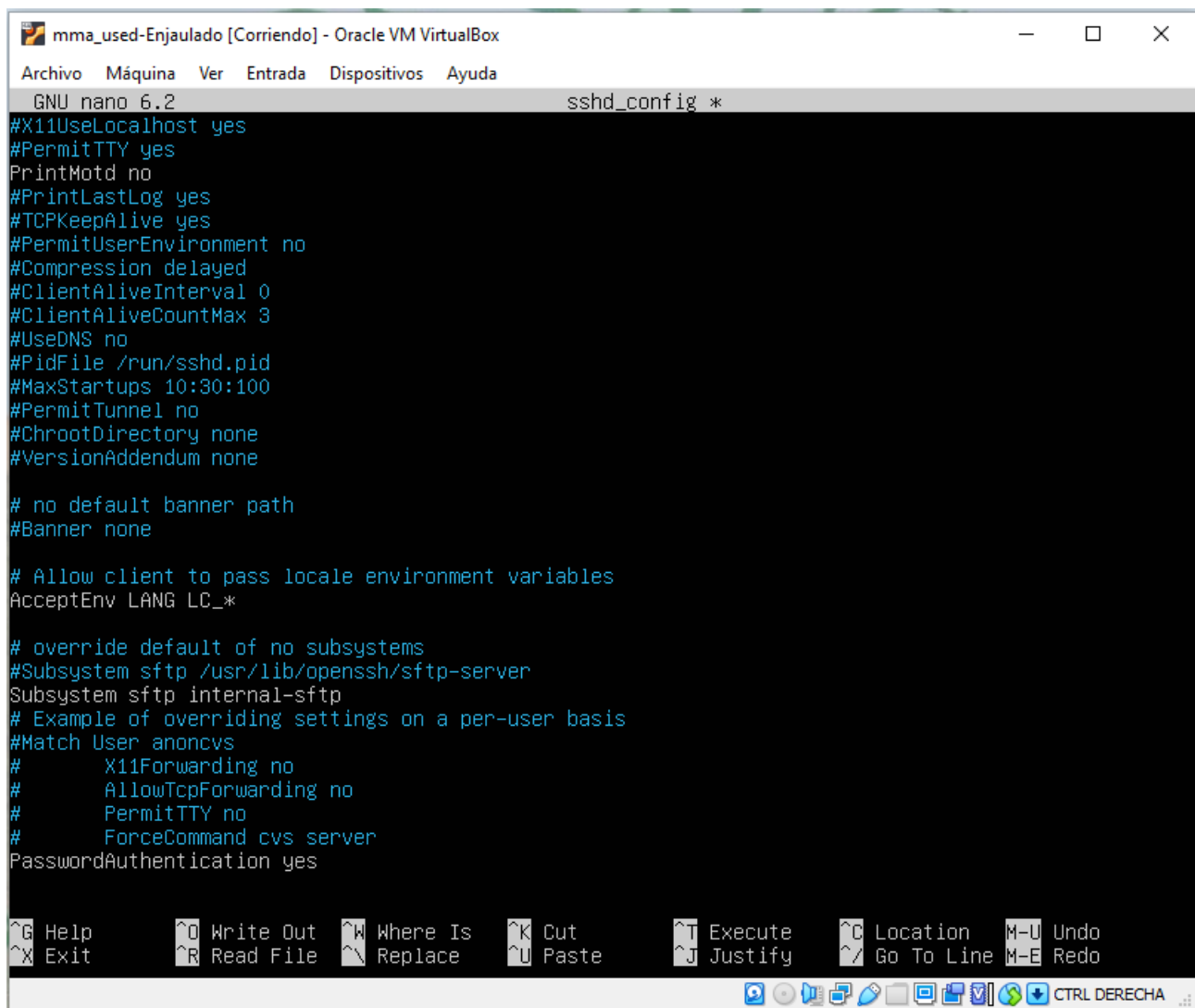
#LoginGraceTime 2m
#PermitRootLogin prohibit-password

miadmin@mma-used:~$ sudo nano /etc/ssh/sshd_config_
```

Para realizar una copia del fichero utilizaremos el comando **cp**.

```
miadmin@mma-used:~$ sudo cp /etc/ss
ssh/ ssl/
miadmin@mma-used:~$ sudo cp /etc/ssh/
moduli      ssh_host_dsa_key      ssh_host_ed25519_key.pub
ssh_config  ssh_host_dsa_key.pub  ssh_host_rsa_key
ssh_config.d/ ssh_host_ecdsa_key  ssh_host_rsa_key.pub
sshd_config ssh_host_ecdsa_key.pub ssh_import_id
sshd_config.d/ ssh_host_ed25519_key
miadmin@mma-used:~$ cd /etc/ssh/ssh
ssh_config.d/ sshd_config.d/
miadmin@mma-used:~$ cd /etc/ssh
miadmin@mma-used:/etc/ssh$ sudo cp sshd_config sshd_config.backup
miadmin@mma-used:/etc/ssh$ _
```

Para editar el fichero utilizaremos el comando **nano**.



The screenshot shows a terminal window titled 'mma\_used-Enjaulado [Corriendo] - Oracle VM VirtualBox'. Inside, the GNU nano 6.2 text editor is open, editing the 'sshd\_config' file. The file content is as follows:

```
GNU nano 6.2 sshd_config *
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

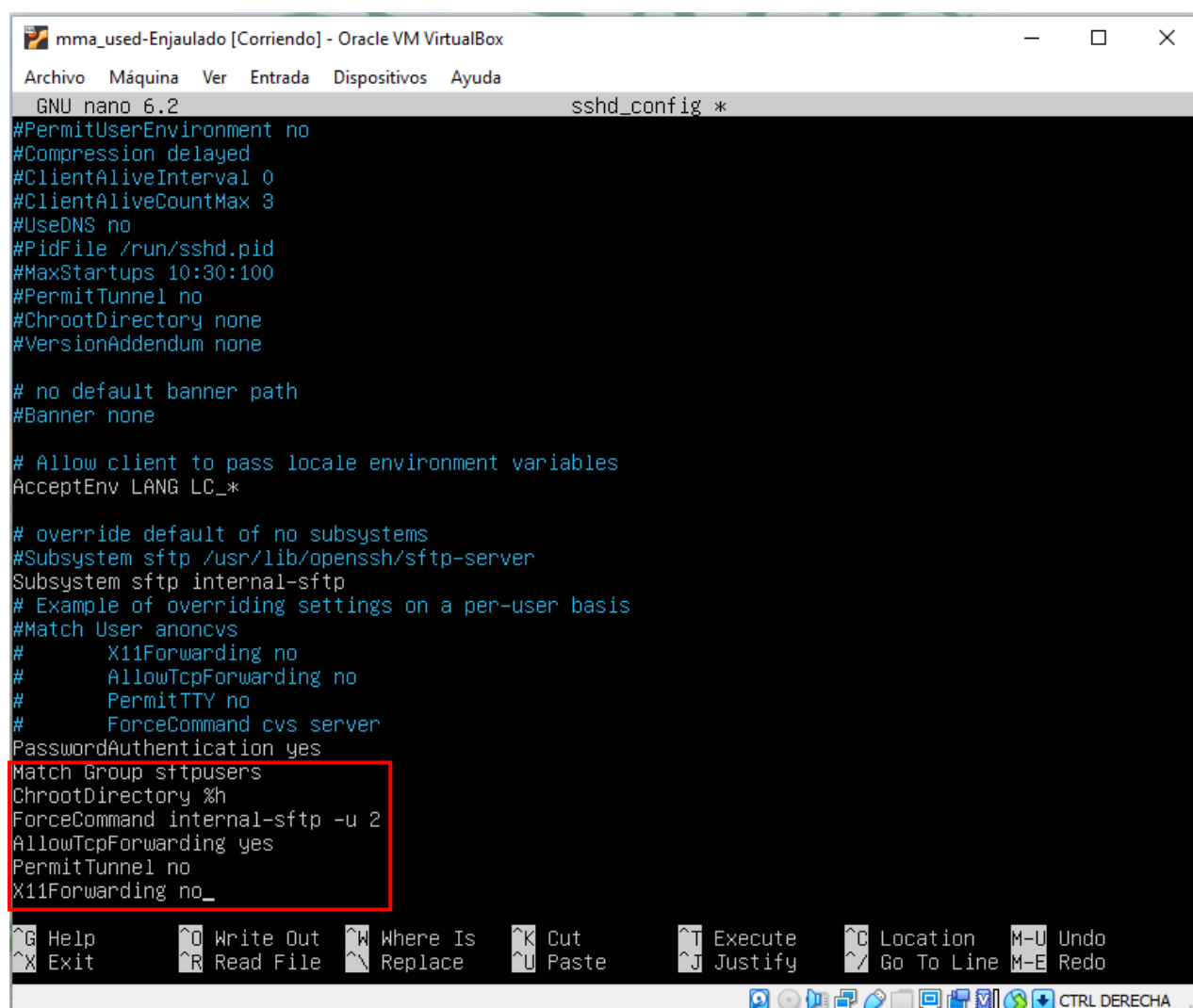
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# 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
```

At the bottom of the window, there is a menu bar with the following options: Help, Write Out, Where Is, Cut, Execute, Location, M-U Undo, Exit, Read File, Replace, Paste, Justify, Go To Line, M-E Redo. A status bar at the very bottom shows 'CTRL DERECHA'.



En el fichero añadiremos las siguientes líneas.



```
mma_used-Enjaulado [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2                                sshd_config *
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

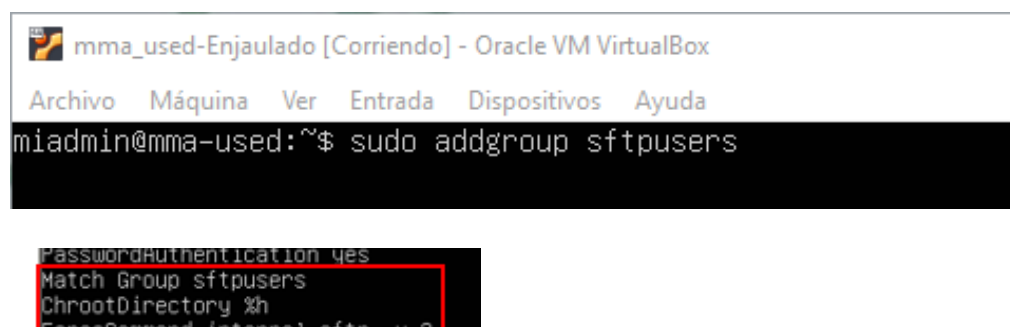
# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# 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 sftpusers
ChrootDirectory %h
ForceCommand internal-sftp -u 2
AllowTcpForwarding yes
PermitTunnel no
X11Forwarding no_

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line   M-E Redo
CTRL DERECHA
```

Cuando lo hayamos escrito, guardaremos el fichero y saldremos de él. Luego, crearemos un grupo mediante el comando **addgroup** con el mismo nombre con el que pusimos en **Match group** del fichero **sshd\_config**.



```
mma_used-Enjaulado [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
miadmin@mma-used:~$ sudo addgroup sftpusers

PasswordAuthentication yes
Match Group sftpusers
ChrootDirectory %h
ForceCommand internal-sftp -u 2
```

Lo siguiente que tenemos que hacer es modificar el usuario y añadirle el grupo que hemos creado previamente, con la opción **-G**.

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
miadmin@mma-used:~$ sudo usermod -a -G sftputers daw201_
```

Para comprobar que todo está bien realizado, nos iremos a **Filezilla**, y cuando nos conectemos al usuario podremos ver cómo está enjaulado en la carpeta **public\_html**, y no podemos acceder al raíz, ya que no tiene permisos para ello.

