

INGENIERÍA DE SERVIDORES (2016-2017)
DOBLE GRADO EN INGENIERÍA INFORMÁTICA Y MATEMÁTICAS
UNIVERSIDAD DE GRANADA

Memoria Práctica 2

Alicia Rodríguez Gómez

April 18, 2017

Contents

1 Cuestión 1	4
1.1 Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes.	4
1.2 ¿Qué ha de hacer para que yum pueda tener acceso a internet en el PC del aula? (Pista: archivo de configuración en /etc, proxy:stargate.ugr.es:3128)	4
1.3 ¿Cómo añadimos un nuevo repositorio?	4
2 Cuestión 2	4
2.1 Liste los argumentos de apt necesarios para instalar, buscar y eleminar paquetes.	4
2.2 ¿Qué ha de hacer para que apt pueda tener acceso a Internet en el PC del aula?(Pista: archivo de configuración en /etc, proxy:stargate.ugr.es:3128) .	5
2.3 ¿Cómo añadimos un nuevo repositorio?	5
3 Cuestión 3	5
3.1 ¿Con qué comando puede abrir/cerrar un puerto usando ufw? Muestre un ejemplo de cómo lo ha hecho.	5
3.2 ¿Con qué comando puede abrir/cerrar un puerto usando firewall-cmd en CentOs? Muestre un ejemplo de cómo lo ha hecho.	6
3.3 Utilice el comando nmap para ver que, efectivamente, los puertos están accesibles.	7
4 Cuestión 4	8
4.1 ¿Qué diferencia hay entre telnet y ssh?	8
5 Cuestión 5	9
5.1 ¿Para qué sirve la opción -X?	9
5.2 Ejecute remotamente, es decir, desde la máquina anfitriona (si tiene Linux) o desde la otra máquina virtual, el comando gedit es una sesión abierta con ssh. ¿Qué ocurre?	9
6 Cuestión 6	10
6.1 Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola remota sin introducir la contraseña. Pruebe que funciona. (Pista: ssh-keygen, ssh-copy-id).	10
7 Cuestión 7	12
7.1 ¿Qué archivo es el que contiene la configuración del servicio ssh? ¿Qué parámetros hay que modificar para evitar que el usuario root acceda? Cambie el puerto por defecto y compruebe que se puede acceder.	12

8 Cuestión 8	14
8.1 Indique si es necesario reiniciar el servicio ¿Cómo se reinicia un servicio en Ubuntu? ¿y en CentOS? Muestre la secuencia de comandos para hacerlo.	14
9 Cuestión 9	14
9.1 Muestre los comandos que ha utilizado en Ubuntu Server y en CentOS (aunque en este último puede utilizar la GUI, en tal caso, realice capturas de pantalla). Compruebe que la instalación ha sido correcta.	14
10 Cuestión 10	17
10.1 Realice la instalación usando GUI o PowerShell y compruebe que el servicio está funcionando accediendo a la MV a través de la anfitriona.	17
11 Cuestión 11	18
11.1 Muestre un ejemplo de uso del comando (p.ej. http://fedoraproject.org/wiki/VMWare)	18
12 Cuestión 12	18
12.1 Realice la instalación de esta aplicación y pruebe a modificar algún parámetro de algún servicio. Muestre las capturas de pantalla pertinentes así como el proceso de instalación.	18
13 Cuestión 13	20
13.1 Instale phpMyAdmin, indique cómo lo ha realizado y muestre algunas capturas de pantalla. Configure PHP para poder importar BDs de hasta 25MiB (en vez de los 8 MiB de límite por defecto). Indique cómo ha realizado el proceso y muestre capturas de pantalla.	20
14 Cuestión 14	23
14.1 Viste al menos una de las webs de los software mencionados y pruebe las demos que ofrecen realizando capturas de pantalla y comentando qué está realizando.	23
15 Cuestión 15	26
15.1 Ejecute los ejemplo de find, grep.	26
15.2 Escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio.	26
15.3 Muestre un ejemplo de uso para awk.	28
16 Cuestión 16	28
16.1 Escriba el script para cambiar el acceso a ssh usando PHP o Python. . . .	28
17 Cuestión 17	29
17.1 Abra una consola de Powershell y pruebe a parar un programa en ejecución (p.ej), realice capturas de pantalla y comente lo que muestra.	29

1 Cuestión 1

1.1 Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes.

Como se muestra en la documentación de Red Hat[10] acerca de yum, para instalar paquetes con el comando yum se debe introducir la siguiente acción: '*yum install <package name/s>*' donde *package name/s* se refiere al nombre del paquete que se quiere instalar. Cuando nos referimos a la búsqueda de paquetes se debe utilizar la siguiente acción: '*yum search <keyword>*' donde *keyword* se refiere a la palabra que se busca entre los paquetes que se tiene. Por último, para la eliminación de paquetes se usa la orden '*yum remove <package name/s>*' donde *package name/s* se refiere al paquete que se quiere eliminar.

Señalar que para que se puedan ejecutar cualquiera de estas acciones se deben tener permisos de superusuario.

1.2 ¿Qué ha de hacer para que yum pueda tener acceso a internet en el PC del aula? (Pista: archivo de configuración en /etc, proxy:stargate.ugr.es:3128)

Para que yum pueda tener acceso a internet[6] hay que acceder al archivo de configuración de yum. Este se encuentra en la ruta /etc/yum.conf. Uno de los parámetros de este archivo es proxy y basta con escribir en este *proxy:stargate.ugr.es:3128* para que yum tenga acceso a internet en el PC del aula.

1.3 ¿Cómo añadimos un nuevo repositorio?

Como se explica en la documentación de Red Hat[11], para añadir un nuevo repositorio a yum se debe añadir una sección [repository] al archivo .repo que se encuentra en el directorio '/etc/yum.repos.d/'.

Otra alternativa para añadir un nuevo repositorio y al mismo tiempo habilitarlo sería con la ejecución del siguiente comando: *yum-config-manager -add-repo repository_url* donde *repository_url* se trata de la url donde el archivo .repo que se quiere añadir.

2 Cuestión 2

2.1 Liste los argumentos de apt necesarios para instalar, buscar y eleminar paquetes.

Utilizando la orden la línea de comandos 'man apt' se puede leer que los argumentos de apt para la instalación de un paquete es '*sudo apt-get install <package name/s>*' donde *package name/s* se refiere al nombre del paquete o de los paquetes que se quieren instalar.

Por otro lado, si lo que se quiere es buscar paquetes con apt se utiliza la orden '*sudo apt-cache search <keyword>*' donde keyword se refiere a la palabra que puede identificarse en el paquete o paquetes que queremos encontrar. Por último, si lo que se quiere es eliminar un paquete se debe utilizar el siguiente comando '*sudo apt-get remove <package name/s>*' donde package name/s se refiere a el paquete o lista de paquetes que se quieren eliminar.

2.2 ¿Qué ha de hacer para que apt pueda tener acceso a Internet en el PC del aula?(Pista: archivo de configuración en /etc, proxy:stargate.ugr.es:3128)

Para que apt pueda tener acceso a internet[7] desde el PC del aula hay que acceder al archivo de configuración de apt. Este se encuentra en la ruta /etc/apt/apt.conf. Cuando tengamos dicho archivo abierto basta con añadir la línea siguiente: *Acquire::http::Proxy "stargate.ugr.es:3128"*. Tras esto ya debe tener apt acceso a internet.

2.3 ¿Cómo añadimos un nuevo repositorio?

Para añadir un nuevo repositorio debemos utilizar la siguiente orden: '*sudo add-apt-repository REPOSITORY*' donde REPOSITORY se refiere al nombre del repositorio. Como explica en el manual de Ubuntu[9] este repositorio queda almacenado en el directorio /etc/apt/sources.list.d .

3 Cuestión 3

3.1 ¿Con qué comando puede abrir/cerrar un puerto usando ufw? Muestre un ejemplo de cómo lo ha hecho.

Como se muestra en el manual de Ubuntu[8] o también tecleando en el terminal '*man ufw*', para abrir un puerto usando el comando ufw habría que hacer lo siguiente; en primer lugar ponerte en modo *su* y seguidamente introducir en la línea de comandos lo siguiente: *ufw allow ARGS* donde ARGS es el número del puerto que queremos abrir. Análogamente al proceso de abrir un puerto, nos podemos encontrar con la necesidad de cerrar un puerto previamente abierto. Para ello, en el manual citado anteriormente, encontramos que el comando que te permite cerrar un puerto usando ufw es: *ufw deny ARGS* donde, como hemos mencionado anteriormente, ARGS es el número del puerto que queremos cerrar.

A continuación, veamos unas imágenes donde se abre y se cierra un puerto , en este caso hemos utilizado el puerto 22 que se corresponde con el servicio ssh:

```
root@server-raid:/home/aliciarg# 
root@server-raid:/home/aliciarg# 
root@server-raid:/home/aliciarg# 
root@server-raid:/home/aliciarg# 
root@server-raid:/home/aliciarg# 
root@server-raid:/home/aliciarg# ufw status
Estado: activo
root@server-raid:/home/aliciarg# ufw allow 22
Regla añadida
Regla añadida (v6)
root@server-raid:/home/aliciarg# ufw status
Estado: activo

Hasta          Acción      Desde
----          ----      -----
22            ALLOW      Anywhere
22 (v6)        ALLOW      Anywhere (v6)

root@server-raid:/home/aliciarg# ufw deny 22
Regla actualizada
Regla actualizada (v6)
root@server-raid:/home/aliciarg# ufw status
Estado: activo

Hasta          Acción      Desde
----          ----      -----
22            DENY      Anywhere
22 (v6)        DENY      Anywhere (v6)

root@server-raid:/home/aliciarg#
```

Figure 3.1: Captura de la ejecución del comando ufw para abrir y cerrar un puerto.

3.2 ¿Con qué comando puede abrir/cerrar un puerto usando firewall-cmd en CentOs? Muestre un ejemplo de cómo lo ha hecho.

Consultando en el manual de firewall-cmd (man firewall-cmd) observamos que los parámetros para que este comando pueda abrir un puerto es `-add-port=portid/protocol` y para cerrarlo `-remove-port=portid/protocol`. A continuación se muestra la captura de como se ha ejecutado.

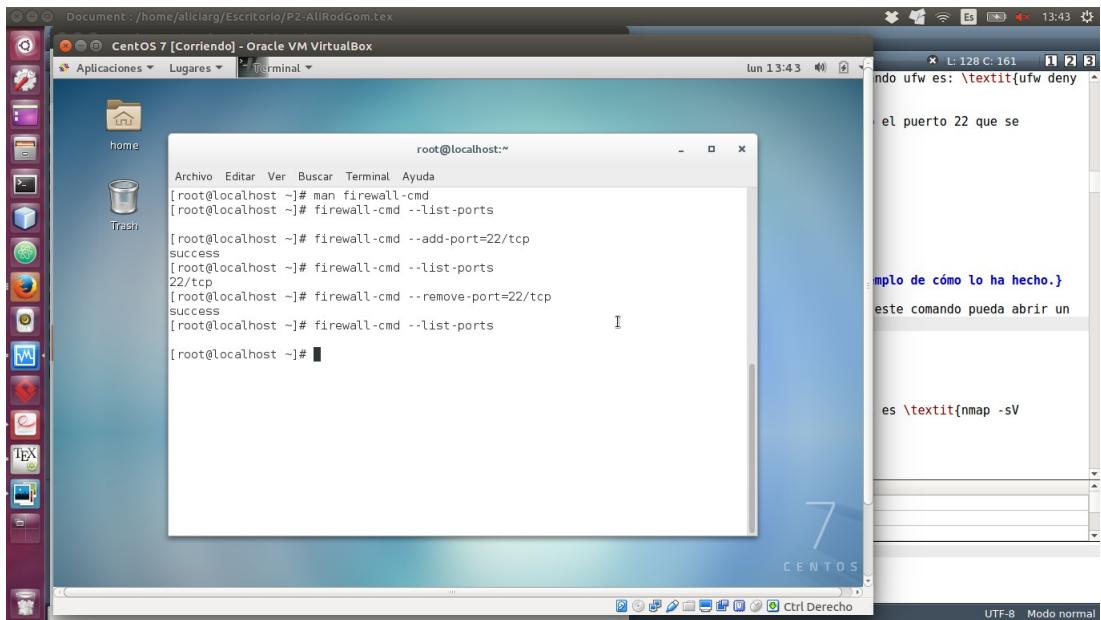


Figure 3.2: Captura de la ejecución del comando `firewall-cmd` para abrir y cerrar un puerto.

3.3 Utilice el comando nmap para ver que, efectivamente, los puertos están accesibles.

Consultando el manual de `nmap`, comprobamos que el comando para ver los puertos accesibles en tu pc local es `nmap -sV localhost`. A continuación veamos la ejecución de dicho comando:

```

nmap done. 0 IP addresses (0 hosts up) scanned in 6.12 seconds
aliciarg@server-raid lun abr 10 2017 :~$ nmap -sV localhost

Starting Nmap 6.40 ( http://nmap.org ) at 2017-04-10 18:43 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00050s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      (protocol 2.0)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/service-
submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=4/10%Time=58EBB62E%P=x86_64-pc-linux-gnu%R(NULL
SF:,2B,"SSH-2\0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\.8\r\n");
Service detection performed. Please report any incorrect results at http://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.18 seconds
aliciarg@server-raid lun abr 10 2017 :~$
```

Figure 3.3: Captura de la ejecución del comando nmap para ver que puertos están accesibles. En este caso se observa que el único puerto accesible es el 22 que se corresponde con el servicio ssh.

4 Cuestión 4

4.1 ¿Qué diferencia hay entre telnet y ssh?

Como se explica en el sitio web oficial de *ssh*[17], tanto telnet y ssh son protocolos de acceso remoto mediante Internet. Telnet es anterior a ssh, y se trata de un protocolo cliente-servidor que proporciona al usuario una terminal del host remoto mediante la aplicación cliente telnet. El problema de este protocolo aparece en términos de seguridad, dado que el protocolo no cifra la conexión entre el cliente y el servidor telnet. Por lo tanto cualquier persona con un simple software de depuración de red puede acceder al flujo de datos de la conexión telnet y capturas datos tan sensibles como usuario y contraseña de la conexión.

Sin embargo, ssh(*Secure Shell*) soluciona el problema de seguridad que rodea a telnet, es decir, protege las identidades, contraseñas y datos del usuario frente a posibles ataques que se puedan sufrir en la red. Por lo tanto, aunque telnet apareció anteriormente como protocolo de red para el acceso remoto, ha sido mayormente reemplazado por el protocolo ssh debido a las mejoras en seguridad que este último proporciona.

5 Cuestión 5

5.1 ¿Para qué sirve la opción -X?

Consultando en *man ssh* podemos saber que la opción ssh -X te permite activar el reenvío X11. El reenvío X11 es una técnica que proporciona una interfaz gráfica segura.

5.2 Ejecute remotamente, es decir, desde la máquina anfitriona (si tiene Linux) o desde la otra máquina virtual, el comando gedit es una sesión abierta con ssh. ¿Qué ocurre?

Cuando ejecutamos el comando gedit desde mi máquina anfitriona, cuyo sistema operativo es Ubuntu, nos aparece el siguiente *warning*:

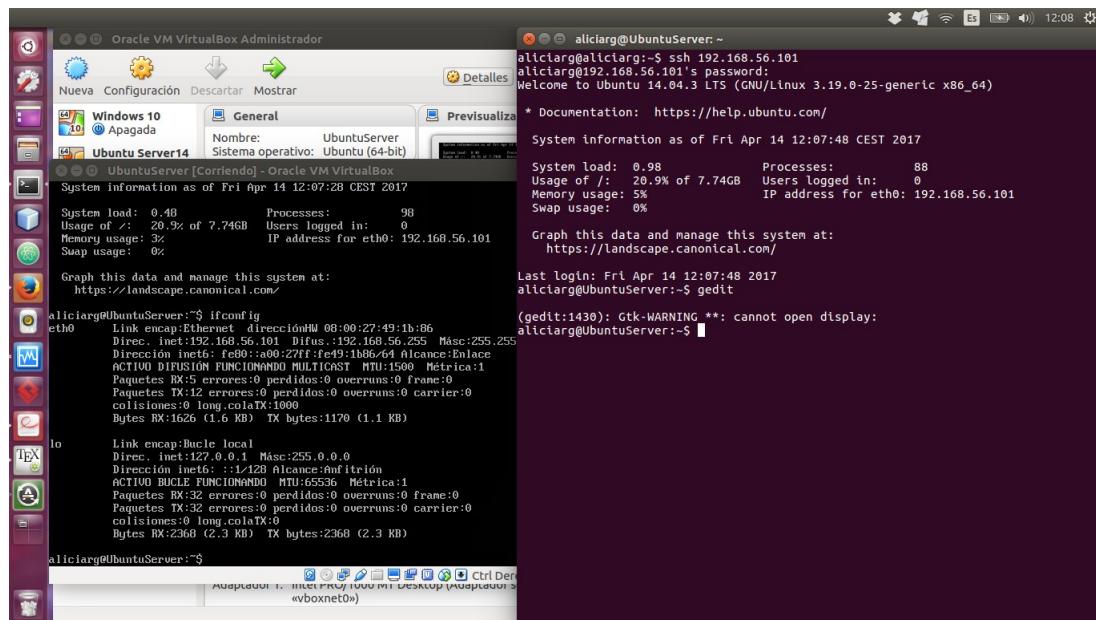


Figure 5.1: Ejecución del comando gedit desde la máquina anfitriona

El hecho de que no se pueda ejecutar es porque por defecto la conexión ssh no proporciona una interfaz gráfica, sin embargo veamos a continuación que si establecemos la conexión ssh con la opción -X, que esta nos proporciona un interfaz gráfica de usuario, entonces si que se nos abrirá la ventana de gedit.

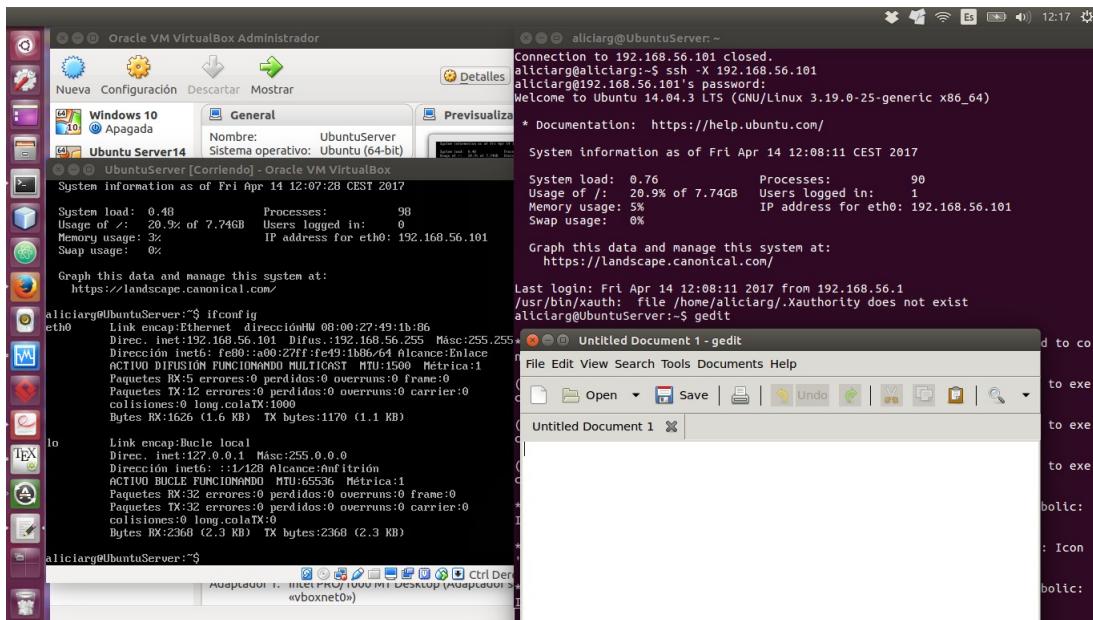


Figure 5.2: Conexión ssh con la opción -X que proporciona una interfaz gráfica.

6 Cuestión 6

6.1 Muestre la secuencia de comandos y las modificaciones a los archivos correspondientes para permitir acceder a la consola remota sin introducir la contraseña. Pruebe que funciona. (Pista: ssh-keygen, ssh-copy-id).

Para acceder a la consola remota sin introducir la contraseña debemos seguir las siguientes instrucciones[12][2]:

1. Ejecutamos el comando **ssh-keygen**, el cual no especificamos con **-t** el tipo de llave que se quiere ya que la que genera por defecto es la que se quiere. El comando se ejecuta en el equipo que actuará como cliente del servicio, es decir, en mi caso se trata de mi máquina local cuyo sistema operativo es Ubuntu 16.04.2. Aquí hemos generado ya la clave pública.
2. Seguidamente ejecutamos el comando **ssh-copy-id aliciarg@192.168.56.101** donde aliciarg es el nombre de usuario del servidor y 192.168.56.101 es la IP del mismo.

```

aliciarg@aliciarg:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/aliciarg/.ssh/id_rsa):
/home/aliciarg/.ssh/id_rsa already exists.
Overwrite (y/n)?
aliciarg@aliciarg:~$ ssh-copy-id aliciarg@192.168.56.101
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
aliciarg@192.168.56.101's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'aliciarg@192.168.56.101'"
and check to make sure that only the key(s) you wanted were added.

aliciarg@aliciarg:~$ 

```

Figure 6.1: Comandos para permitir acceder a la consola remota sin introducir contraseña

A continuación, mostramos un ejemplo de un acceso en el que no se requiere la contraseña

```

aliciarg@UbuntuServer:~$
(gedit:1544): dconf-WARNING **: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No existe el archivo o el directorio)
aliciarg@UbuntuServer:~$ exit
logout
Connection to 192.168.56.101 closed.
aliciarg@aliciarg:~$ clear

aliciarg@aliciarg:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/aliciarg/.ssh/id_rsa):
/home/aliciarg/.ssh/id_rsa already exists.
Overwrite (y/n)?
aliciarg@aliciarg:~$ ssh-copy-id aliciarg@192.168.56.101
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
aliciarg@192.168.56.101's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'aliciarg@192.168.56.101'"
and check to make sure that only the key(s) you wanted were added.

aliciarg@aliciarg:~$ ssh 192.168.56.101
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
System information as of Fri Apr 14 12:23:31 CEST 2017
System load:  0.0          Processes:      83
Usage of /:   20.9% of 7.74GB  Users logged in:    1
Memory usage: 5%
Swap usage:  0%
Graph this data and manage this system at:
https://landscape.canonical.com/
Last login: Fri Apr 14 12:17:05 2017 from 192.168.56.1
aliciarg@UbuntuServer:~$ 

```

Figure 6.2: Comandos para permitir acceder a la consola remota sin introducir contraseña

7 Cuestión 7

7.1 ¿Qué archivo es el que contiene la configuración del servicio ssh?
¿Qué parámetros hay que modificar para evitar que el usuario root acceda? Cambie el puerto por defecto y compruebe que se puede acceder.

El archivo que contiene la configuración ssh[4] del cliente es el archivo *ssh-config*:

```
aliciarg@UbuntuServer:~$ cat /etc/ssh/ssh_config
#
# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.
#
# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file
# 3. system-wide file
#
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.
#
# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# RhostsRSAAuthentication no
# RSAAuthentication yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/identity
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# Port 22
# Protocol 2,1
# Cipher 3des
```

Figure 7.1: Archivo de configuración del servicio ssh

Como nos muestra el sitio web oficial de SSH[1] para evitar que el usuario root acceda hay que modificar la línea del archivo que pone *PermitRootLogin* y ponerle no.

```
GNU nano 2.2.6          Archivo: /etc/ssh/sshd_config          Modificado
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile  %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes
```

Figure 7.2: No permitir que el usuario root acceda a ssh

En el propio archivo de configuración existe un parámetro llamado *port* en el cual actualmente tiene el valor 22, que es el valor por defecto. Basta cambiar ese valor por el nuevo número de puerto que le queremos asignar. En este caso he elegido el puerto 4212.

```
GNU nano 2.2.6           Archivo: /etc/ssh/sshd_config           Modificado
#
# Package generated configuration file
# See the sshd_config(5) manpage for details
#
# What ports, IPs and protocols we listen for
Port 4212
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::1
#ListenAddress 0.0.0.0
Protocol 2
# Hostkeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519.key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys
```

Figure 7.3: Cambiando el puerto 22 por el 4212.

```
aliciarg@UbuntuServer:~$ sudo nano /etc/ssh/sshd_config
aliciarg@UbuntuServer:~$ sudo service ssh restart
ssh stop/waiting
ssh start/running, process 1865
aliciarg@UbuntuServer:~$
```

Figure 7.4: Reiniciando el servicio ssh para que se efectúen los cambios.

```
aliciarg@aliciarg:~$ ssh -p 4212 192.168.56.101
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
 * System information as of Fri Apr 14 12:41:35 CEST 2017
System load:  0.0          Processes:      83
Usage of /:  20.9% of 7.74GB  Users logged in:   1
Memory usage: 5%          IP address for eth0: 192.168.56.101
Swap usage:  0%
Graph this data and manage this system at:
  https://landscape.canonical.com/
Last login: Fri Apr 14 12:41:36 2017 from 192.168.56.1
aliciarg@UbuntuServer:~$
```

Figure 7.5: Accediendo al servicio ssh desde el nuevo puerto de escucha.

8 Cuestión 8

- 8.1 Indique si es necesario reiniciar el servicio ¿Cómo se reinicia un servicio en Ubuntu? ¿y en CentOS? Muestre la secuencia de comandos para hacerlo.**

En cualquier tipo de servicio, por lo tanto en el caso de ssh ocurre lo mismo, es necesario reiniciar el servicio tras hacer cualquier tipo de cambios que afecten a la configuración del servicio que corresponda. Por lo tanto la respuesta es afirmativa. Dependiendo del sistema operativo utilizado el reinicio se ejecuta con diferentes comandos. Como se ha mostrado en el ejercicio anterior, en Ubuntu el servicio se reinicia con el comando *sudo service ssh restart*[14]. Por otro lado en CentOS, *sudo systemctl restart sshd* es el comando necesario para reiniciar el servicio ssh[13].

9 Cuestión 9

- 9.1 Muestre los comandos que ha utilizado en Ubuntu Server y en CentOS (aunque en este último puede utilizar la GUI, en tal caso, realice capturas de pantalla). Compruebe que la instalación ha sido correcta.**

Comenzaremos explicando como se ha hecho la instalación en Ubuntu Server. En primer lugar, vamos a instalar Apache para ello utilizaremos el comando **sudo apt-get install apache2**. Seguidamente vamos a instalar MySQL, basta con introducir el comando **sudo apt-get install mysql-server php5-mysql**. En este paso te pide asignarle a la base de datos un clave seguro, aunque esta puede ser la misma que root en mi caso personal he preferido ponerle una nueva. El primer paquete que hemos instalado **mysql-server** instala el servidor sql y el segundo dara soporte PHP a la base de datos instalada. Finalmente para la instalación de PHP debemos ejecutar el comando **sudo apt-get install php5 libapache2-mod-php5 php5-mcrypt**.

Veamos que apache ha sido instalado correctamente, para ello utilizamos el comando **curl http://192.168.1.3 > url** y posteriormente abrimos el archivo url con el comando **nano url** y vemos a continuación que aparece la página por defecto de Apache:

```

alicriarg@server-raid mié abr 12 2017 :~$ ifconfig
eth0      Link encap:Ethernet  direcciónHW 08:00:27:c2:e2:79
          Direc. inet:192.168.1.3  Difus.:192.168.1.255  Másc:255.255.255.0
          Dirección inet6: fe00::a00:27ff:fe2:c2e2/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500  Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:32 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long_colatX:1000
          Bytes RX:0 (0.0 B)  TX bytes:2088 (2.0 KB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO MTU:65536  Métrica:1
          Paquetes RX:36 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:36 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long_colatX:0
          Bytes RX:26158 (26.1 KB)  TX bytes:26158 (26.1 KB)

alicriarg@server-raid mié abr 12 2017 :~$ curl http://192.168.1.3 > url
  % Total    % Received   % Xferd  Average Speed   Time     Time   Current
     0     0     0     0      0k/s   0:--:--:--:--:--:--:-- 10.9M
100 11510  100 11510  0     0 6085k  0:--:--:--:--:--:--:-- 10.9M
alicriarg@server-raid mié abr 12 2017 :~$ nano url_

```

Figure 9.1: Captura de la comprobación de la ip.

```

GNU nano 2.2.6           Archivo: url

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2014-03-19
See: https://launchpad.net/bugs/1288690
-->
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>Apache2 Ubuntu Default Page: It works</title>
  <style type="text/css" media="screen">
    *
      margin: 0px 0px 0px 0px;
      padding: 0px 0px 0px 0px;
    }

    body, html {
      padding: 3px 3px 3px 3px;
      background-color: #D9DBE2;

      font-family: Verdana, sans-serif;
      font-size: 11pt;
      text-align: center;
    }
  </style>
</head>
<body>
  <h1>It works</h1>
  <p>This is the default web page for this server.<br/>
  The Apache2 web server<br/>
  Version 2.4.17 (Ubuntu)<br/>
  It works!</p>
</body>

```

Figure 9.2: Captura de la página web de Apache.

Para el caso de la instalación en CentOS 7, aunque en la memoria da la posibilidad de que su instalación se haga a través de la GUI, en este caso yo lo he instalado a través de comandos en la consola. Para su instalación he seguido los siguientes pasos:

1. **sudo yum -y install httpd**, comando que permite instalar Apache.

2. **sudo firewall-cmd –permanent –add-port=80/tcp**, que como se ha explicado en el ejercicio 3 permite asignar al servicio http el puerto 80 que es su puerto por defecto.
3. **sudo firewall-cmd –reload**, recargamos el firewall. Con estos pasos ya hemos conseguido instalar Apache en CentOS 7. A continuación instalaremos el resto de servicios requeridos.
4. **sudo yum -y install mariadb-server mariadb**, permite instalar el paquete MariaDB.
5. **sudo systemctl start mariadb.service** y **sudo systemctl enable mariadb.service**, comandos que nos servirán para activar el servicio.
6. **sudo yum -y install php**, con este último comando instalamos el paquete php. Con este conseguimos instalar los paquetes que nos faltaban.
7. **sudo systemctl restart httpd**, finalmente nos sirve para recargar el servicio Apache.

Veamos en la siguiente imagen como Apache funciona en centOS.

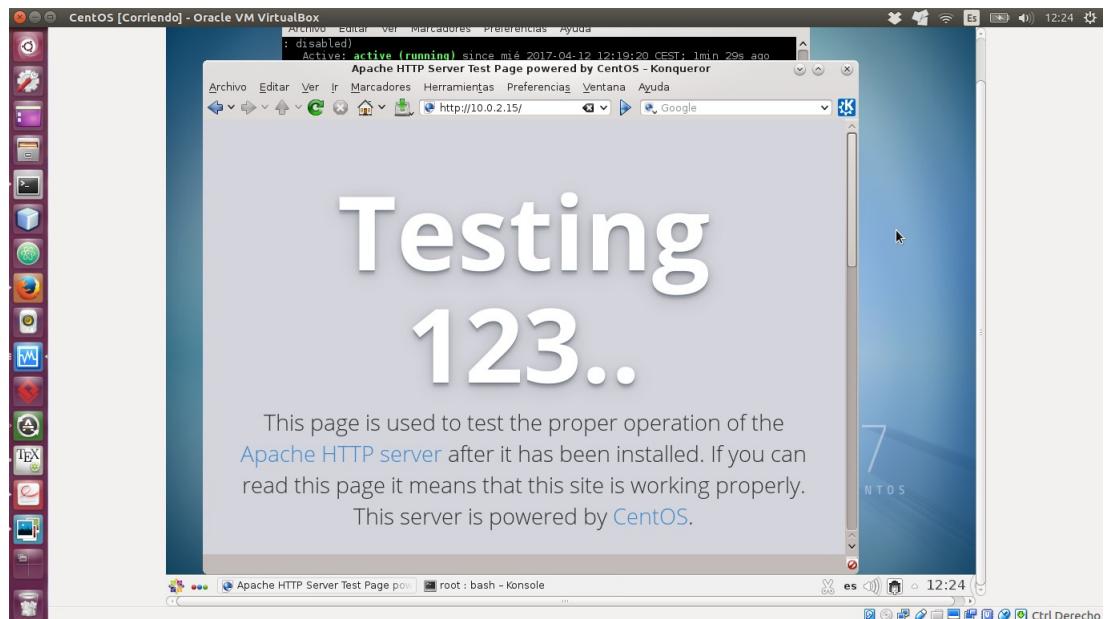


Figure 9.3: Apache funcionando en centOS 7

10 Cuestión 10

10.1 Realice la instalación usando GUI o PowerShell y compruebe que el servicio está funcionando accediendo a la MV a través de la anfitriona.

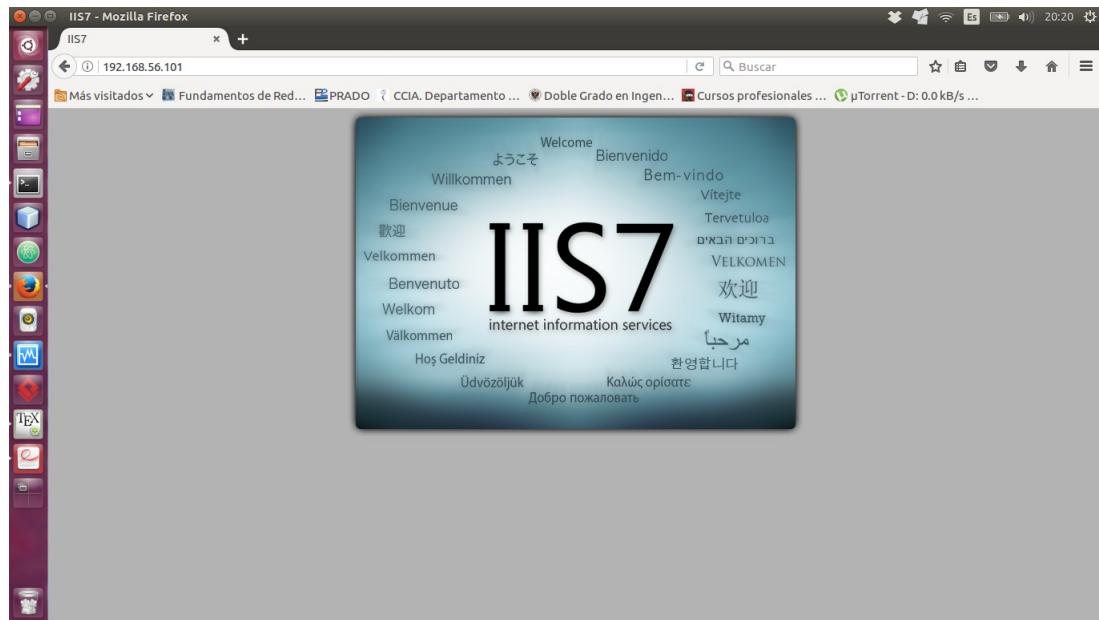


Figure 10.1: Captura de la conexión desde la máquina anfitriona, al servidor web instalado en Windows Server 2008 r2.

Para comprobar que efectivamente se trata del servidor web instalado en mi Windows Server ejecutaremos en el terminal el comando ipconfig y se verifica que es la misma IP.

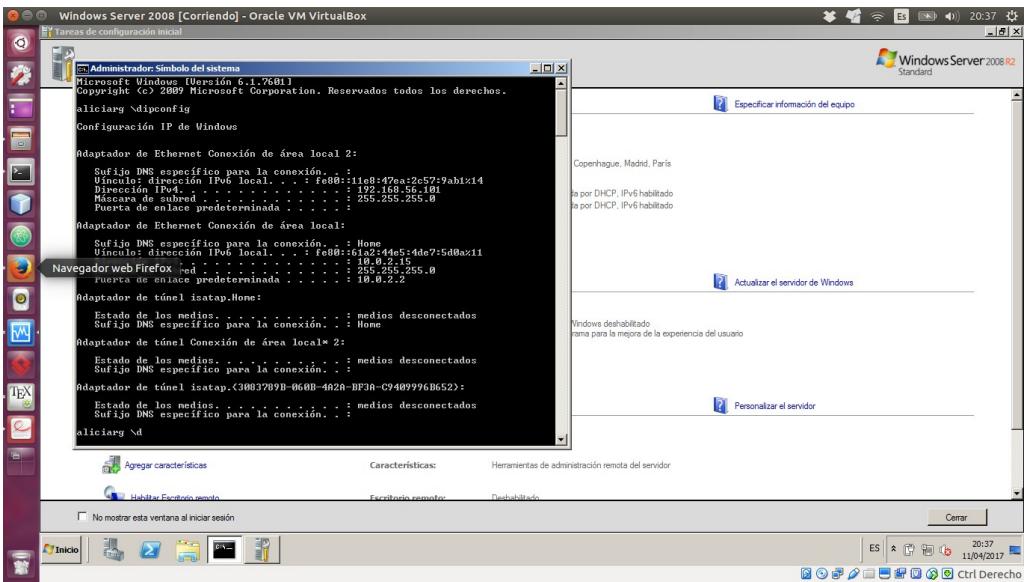


Figure 10.2: Captura de la consulta de la ip de Windows Server 2008 r2.

11 Cuestión 11

11.1 Muestre un ejemplo de uso del comando (p.ej. <http://fedoraproject.org/wiki/VMWare>)

Un ejemplo de uso del comando patch podría ser similar al dado por la referencia[16]. Por ejemplo, en <https://www.drupal.org/patch/apply> vemos como se usa el comando patch. La orden **patch -p1 < patch/file.patch** cuyo argumento -p1 indica que se elimina un directorio de la ruta.

12 Cuestión 12

12.1 Realice la instalación de esta aplicación y pruebe a modificar algún parámetro de algún servicio. Muestre las capturas de pantalla pertinentes así como el proceso de instalación.

El primer paso es descargar la aplicación. En el sitio web oficial[3] aparecen los comandos para descargarte dicha aplicación. Se ejecutan en el servidor, en mi caso en Ubuntu Server, los siguientes comandos:

1. wget http://prdownloads.sourceforge.net/webadmin/webadmin_1.831_all.deb

2. sudo dpkg -i webmin_1.831_all.deb

Así queda instalada la aplicación instalada. Para comprobar que funciona, desde la máquina anfitriona nos conectamos a la siguiente URL <https://192.168.56.101:10000>. Para acceder necesitas identificarte con tu usuario y contraseña del servidor.

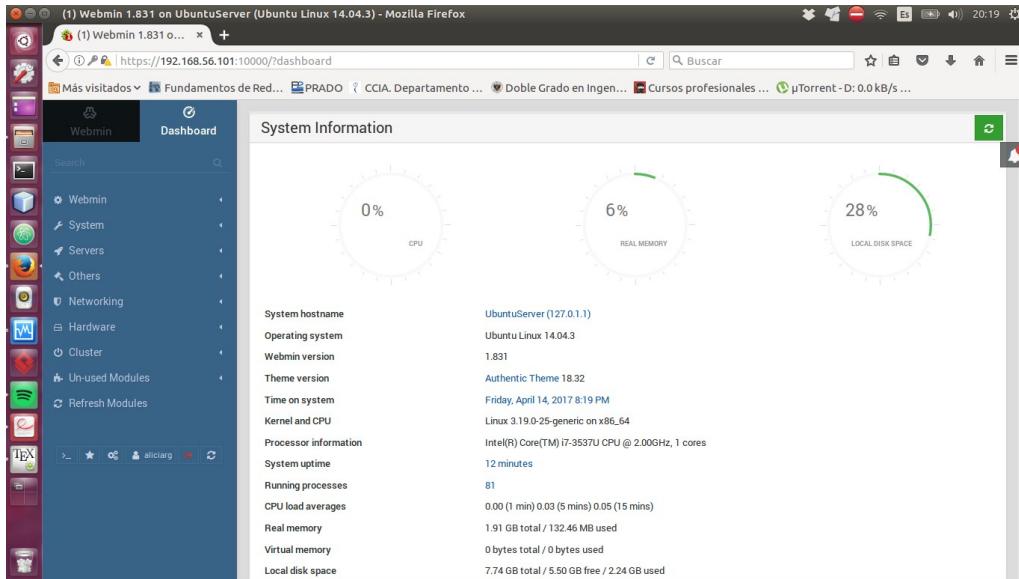


Figure 12.1: Aplicación Webmin instalada y conectada a Ubuntu Server

Desde esta aplicación podemos acceder cualquier tipo de operación que podríamos hacer desde el servidor. Por ejemplo acceder a los datos del usuario que está conectado que en este caso es *aliciarg*, cambiar el nombre de usuario. Pondremos como nuevo nombre de usuario **aliciarodgom**

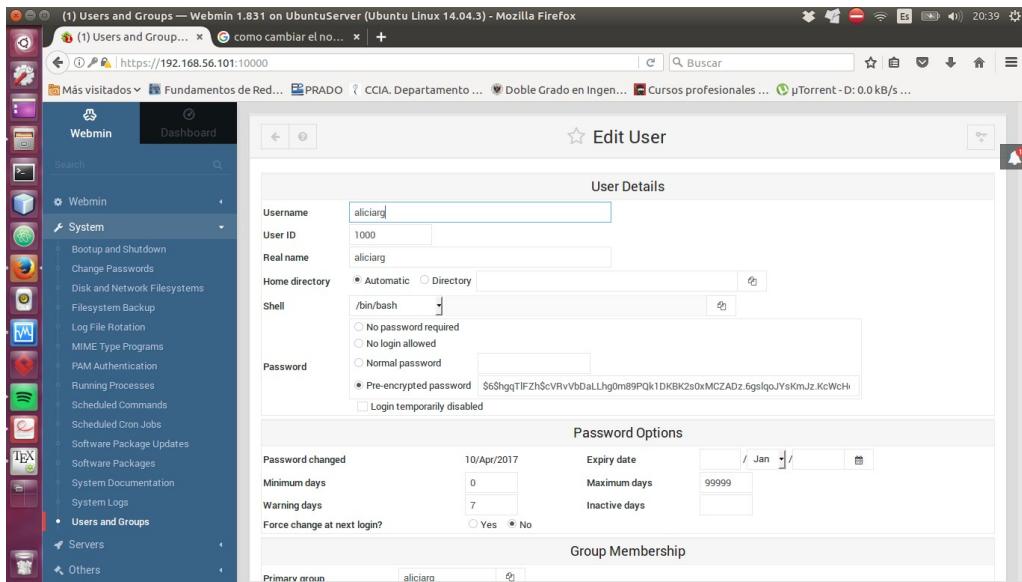


Figure 12.2: Datos del usuario del servidor de Ubuntu Server

```

UbuntuServer login: aliciarg
Password:
Login incorrect
UbuntuServer login: aliciarg
Password:
Login incorrect
UbuntuServer login: aliciargodgon
Password:
Last login: Fri Apr 14 20:06:30 CEST 2017 on ttym1
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation: https://help.ubuntu.com/
System information as of Fri Apr 14 20:48:09 CEST 2017
System load: 0.96      Processes:      89
Usage of /: 24.0% of 7.74GB  Users logged in: 0
Memory usage: 3%
Swap usage: 0%

Graph this data and manage this system at:
https://landscape.canonical.com/
158 packages can be updated.
90 updates are security updates.

aliciarodgon@UbuntuServer:~$ 

```

Figure 12.3: Verificamos como ha cambiado el nombre de usuario.

13 Cuestión 13

13.1 Instale phpMyAdmin, indique cómo lo ha realizado y muestre algunas capturas de pantalla. Configure PHP para poder importar BDs de hasta 25MiB (en vez de los 8 MiB de límite por defecto). Indique cómo ha realizado el proceso y muestre capturas de pantalla.

Para instalar phpMyAdmin, basta con ejecutar el comando **sudo apt-get install phpmyadmin** en el servidor. Durante su instalación nos piden que elijamos el servidor web

que ejecutará phpMyAdmin. En este caso he seleccionado Apache2.



Figure 13.1: Elección del servidor web que soportará phpMyAdmin

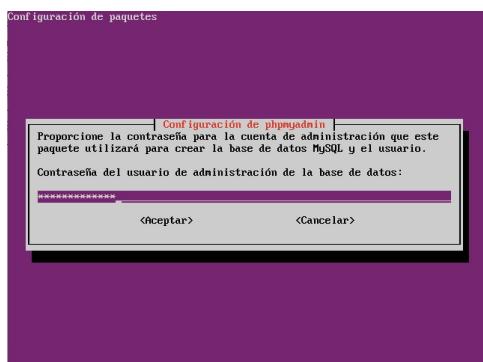


Figure 13.2: Introducción de la contraseña para la base de datos

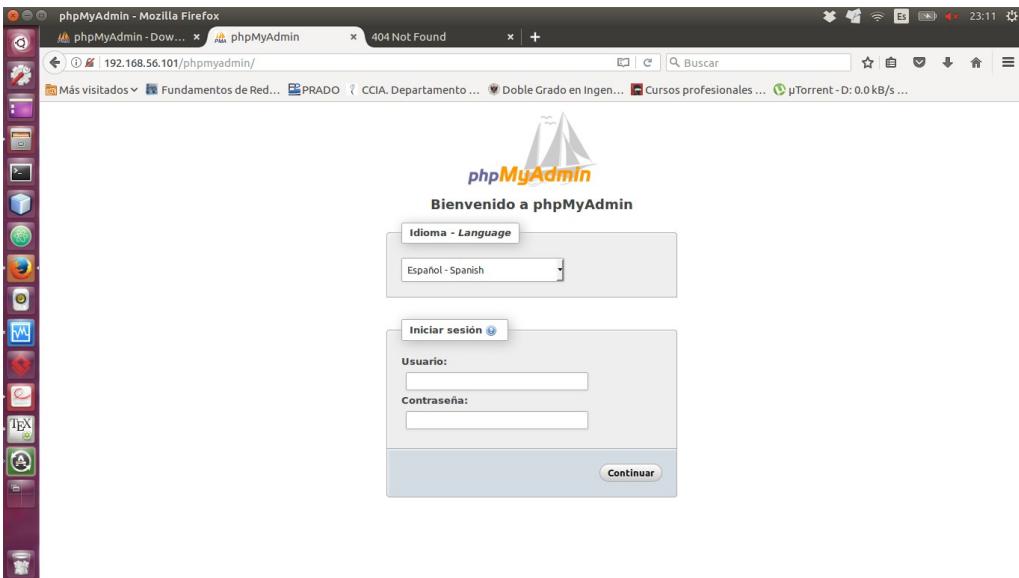


Figure 13.3: Acceso a phpMyAdmin instalado en el servidor Ubuntu Server

Para cambiar el tamaño de las bases de datos que se pueden importar, accedemos al archivo de configuración de php[15]. Para ello utilizamos el comando **sudo nano /etc/php5/cli/php.ini**.

```
UbuntuServer [Corriendo] - Oracle VM VirtualBox
GNU nano 2.2.6           Archivo: /etc/php5/cli/php.ini          Modificado

; POST data will be through the php://input stream wrapper. This can be useful
; to proxy requests or to process the POST data in a memory efficient fashion.
; http://php.net/enable-post-data-reading
;enable_post_data_reading = Off

; Maximum size of POST data that PHP will accept.
; Its value may be 0 to disable the limit. It is ignored if POST data reading
; is disabled through enable_post_data_reading.
; http://php.net/post-max-size
post_max_size = 25M

; Automatically add files before PHP document.
; http://php.net/auto-prepend-file
auto_prepend_file =

; Automatically add files after PHP document.
; http://php.net/auto-append-file
auto_append_file =

; By default, PHP will output a character encoding using
; the Content-type: header. To disable sending of the charset, simply
; set it to be empty.
; http://php.net/default-mimetype
; PHP's built-in default is text/html
; http://php.net/default-mimetype
```

Figure 13.4: Cambiando el valor del tamaño de las BDs a importar a 25MiB

El valor del parámetro *post_max_size* ha sido cambiado a 25 MiB. Tras esto se guardan las modificaciones hechas y se reinicia el servicio. Quedan así los cambios guardados.

14 Cuestión 14

14.1 Viste al menos una de las webs de los software mencionados y pruebe las demos que ofrecen realizando capturas de pantalla y comentando qué está realizando.

En este caso he decidido elegir la web de DirectAdmin, <http://www.directadmin.com/>. En la siguiente imagen se ilustra dicha página web.

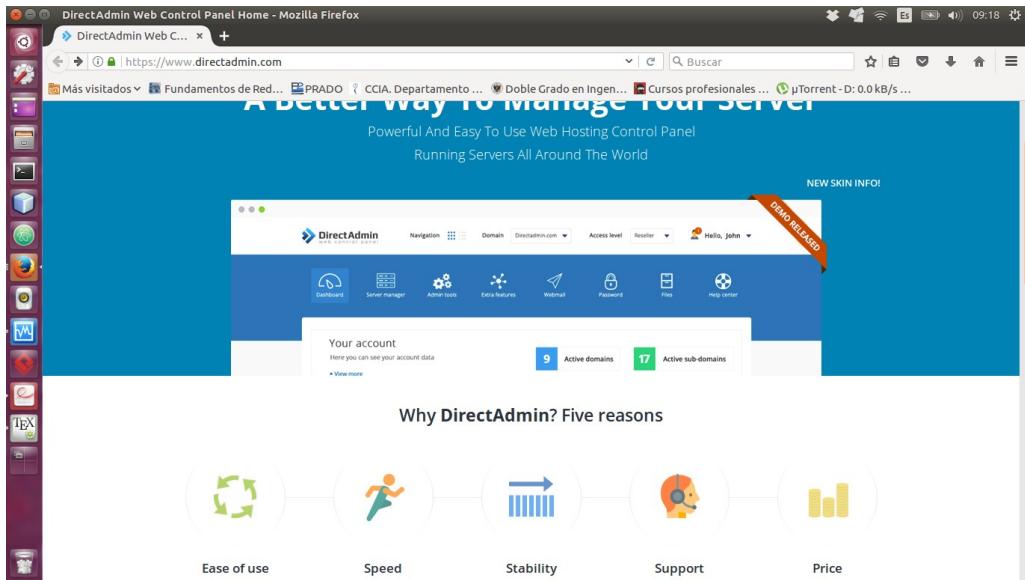


Figure 14.1: Acceso a DirectAdmin

Para probar la demo debemos acceder con alguno de los tres roles que existen, ya sea *Users*, *Resellers* o *Admins*. En este caso yo he utilizado la opción de *Admins Demo*.

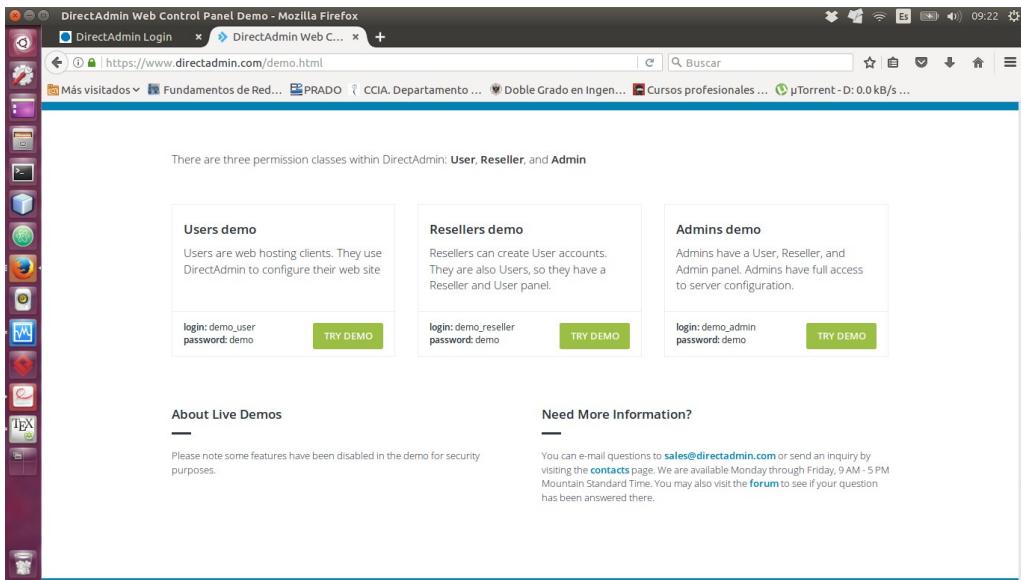


Figure 14.2: *Login and password* para el acceso a la demo

Cuando introducimos el usuario y contraseña que se nos ofrece para la demo de admin, accedemos a la página web principal del software. Esta es la que se puede ver a continuación.

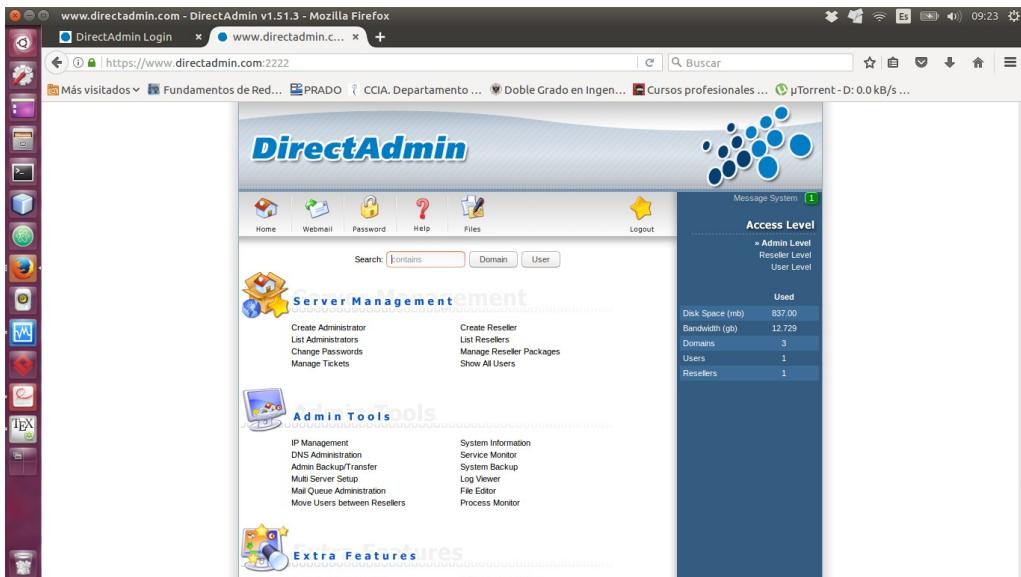


Figure 14.3: Página principal de DirectAdmin

Finalmente, hemos hecho un par de consultas para probar el funcionamiento de la demo.

En primer lugar, he consultado acerca de la información general del sistema, cuyos resultados se pueden ver en la siguiente imagen.

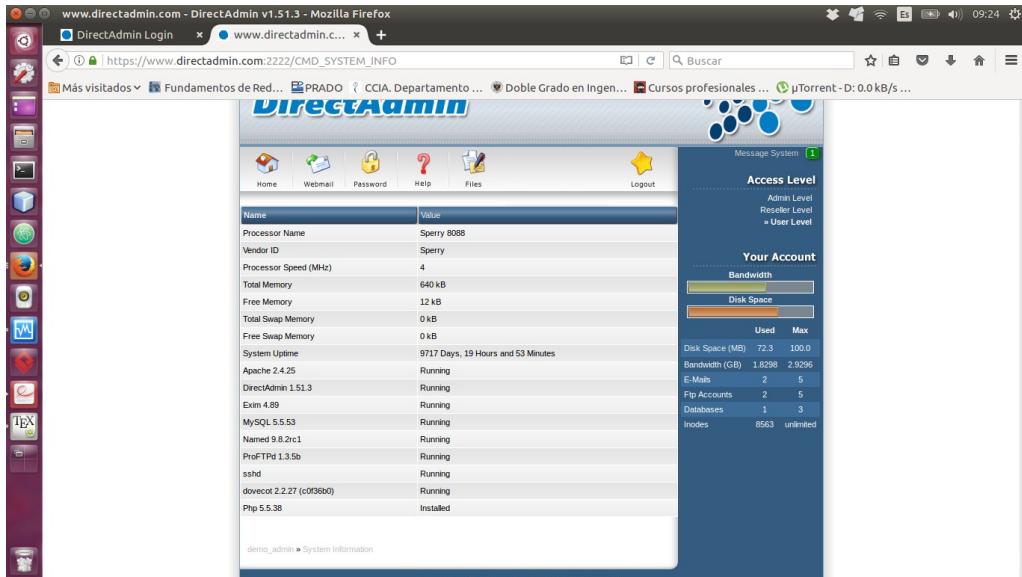


Figure 14.4: Consulta de información acerca del sistema

Seguidamente, he hecho una consulta sobre la IP de DirectAdmin. Dicha consulta se muestra a continuación.

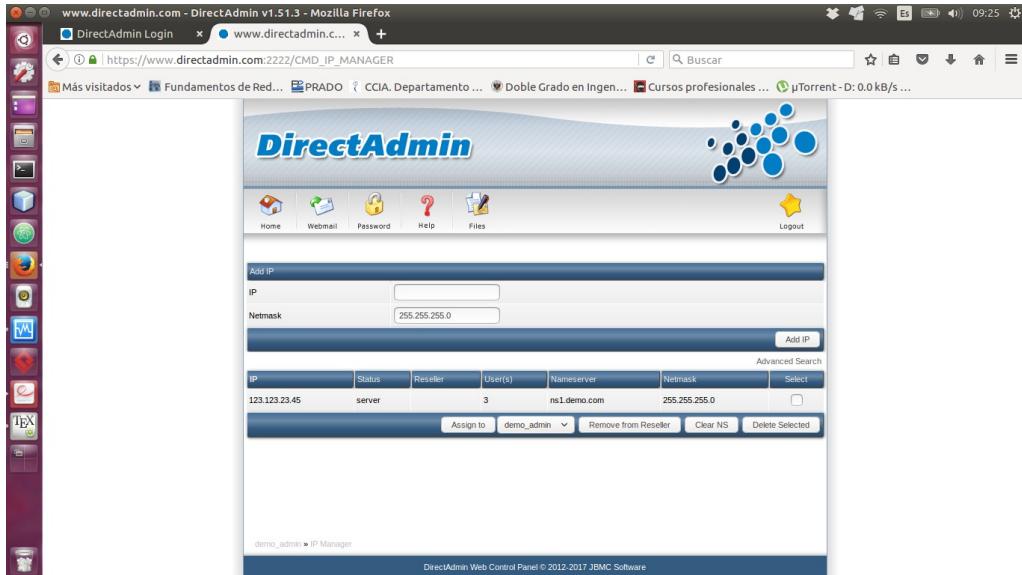


Figure 14.5: Consulta de la IP

Como se ha podido ver en una de las imágenes anterior, el menú de DirectAdmin te proporciona una gran cantidad de acciones que puedes elegir para la consulta y modificación de datos acerca del servidor que quieras controlar.

15 Cuestión 15

15.1 Ejecute los ejemplo de find, grep.

En primer lugar ejecutamos el ejemplo de grep

```
aliciarodgom@UbuntuServer:~$ ps -Af | grep firefox
aliciar+ 3713 1425 0 10:07 tty1    00:00:00 grep --color=auto firefox
aliciarodgom@UbuntuServer:~$
```

Figure 15.1: Información del proceso firefox

Seguidamente ejecutamos el ejemplo de find.

```
aliciarodgom@UbuntuServer:~$ ps -Af | grep firefox
aliciar+ 3713 1425 0 10:07 tty1    00:00:00 grep --color=auto firefox
aliciarodgom@UbuntuServer:~$ find /home/aliciarodgom/ -name '*pdf' -exec cp {} /PDFs \;
aliciarodgom@UbuntuServer:~$ ls /home/aliciarodgom/
!SE restart webmin_1.831_all.deb webmin_1.831_all.deb.1
aliciarodgom@UbuntuServer:~$
```

Figure 15.2: Copia de los archivos pdf en /home/aliciarodgom/PDFs

En este último caso hemos comprobado que no se ha copiado ningún pdf. Esto ocurre porque en la carpeta que hemos buscado, es decir, en /home/aliciarodgom no existe ningún archivo de tipo pdf.

15.2 Escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio.

En primer lugar, he consultado el manual de sed (man sed) para ver las opciones que este propociona. Una vez conocidas sus funcionalidades, he escrito el siguiente script que lo que hace es modificar el puerto de escucha.

```

GNU nano 2.2.6          Archivo: sed.sh

#!/bin/bash

sudo sed -i 's/Port .*/Port 4214/' /etc/ssh/sshd_config
echo "Puerto cambiado"
sudo service ssh restart
echo "Servicio reiniciado"

[ 6 líneas leídas ]

```

Figure 15.3: Script que modifica el puerto de escucha

```

aliciarodgom@UbuntuServer:~$ sudo ./sed.sh
Puerto cambiado
ssh stop/waiting
ssh start/running, process 4295
Servicio reiniciado
aliciarodgom@UbuntuServer:~$
```

Figure 15.4: Ejecución del script

```

GNU nano 2.2.6          Archivo: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 4214
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::

#listenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024
}

# Logging
SyslogFacility AUTH
LogLevel INFO

[ 88 líneas leídas ]

```

Figure 15.5: Comprobamos que efectivamente el puerto de escucha se ha modificado al 4214

15.3 Muestre un ejemplo de uso para awk.

Para conocer el uso del comando awk consultamos su manual (man awk). En este caso voy a utilizar el comando awk para comprobar el puerto de escucha, y se comprobará que efectivamente ha sido modificado en el apartado anterior:

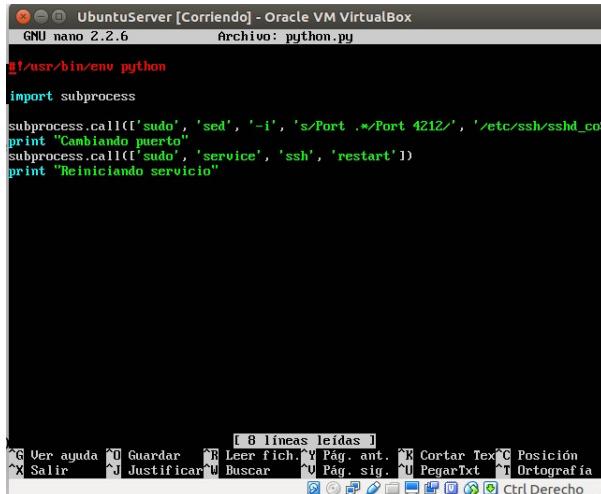
```
aliciarodgom@UbuntuServer:~$ awk '/Port/' /etc/ssh/sshd_config
Port 4214
aliciarodgom@UbuntuServer:~$
```

Figure 15.6: Comprobamos el puerto de escucha

16 Cuestión 16

16.1 Escriba el script para cambiar el acceso a ssh usando PHP o Python.

En primer lugar, para escribir el script en Python debemos instalar[5] este en nuestro servidor. Una vez ya instalado podemos proceder a escribir el archivo en Python. Lo que hará este script será reestablecer el puerto de escucha que tenía antes de modificarlo en el ejercicio anterior, ese puerto era el 4212.



```
GNU nano 2.2.6      Archivo: python.py
#!/usr/bin/env python
import subprocess
subprocess.call(['sudo', 'sed', '-i', 's/Port .*/Port 22/', '/etc/ssh/sshd_config']
print "Cambiando puerto"
subprocess.call(['sudo', 'service', 'ssh', 'restart'])
print "Reiniciando servicio"
```

Figure 16.1: Script en phyton que modifica el puerto de escucha

```

aliciarodgom@UbuntuServer:~$ ./python.py
[sudo] password for aliciarodgom:
Cambiando puerto
ssh stop/waiting
ssh start/running, process 2076
Reinimando servicio
aliciarodgom@UbuntuServer:~$ awk '/Port/' /etc/ssh/sshd_config
Port 4212
aliciarodgom@UbuntuServer:~$ 

```

Figure 16.2: Ejecución del script y comprobación de que el puerto de escucha ha sido modificado correctamente

17 Cuestión 17

17.1 Abra una consola de Powershell y pruebe a parar un programa en ejecución (p.ej), realice capturas de pantalla y comente lo que muestra.

Cuando abrimos la consola de Powershell, lo primero que hacemos es ejecutar el comando *get-process*. Como se muestra en la siguiente imagen nos da un listado de todos los procesos en ejecución junto a características de todos ellos. En este caso, he elegido parar el proceso que corresponde con la consola de Powershell. Para ello ejecuto el comando *stop-process -ID 2320*.

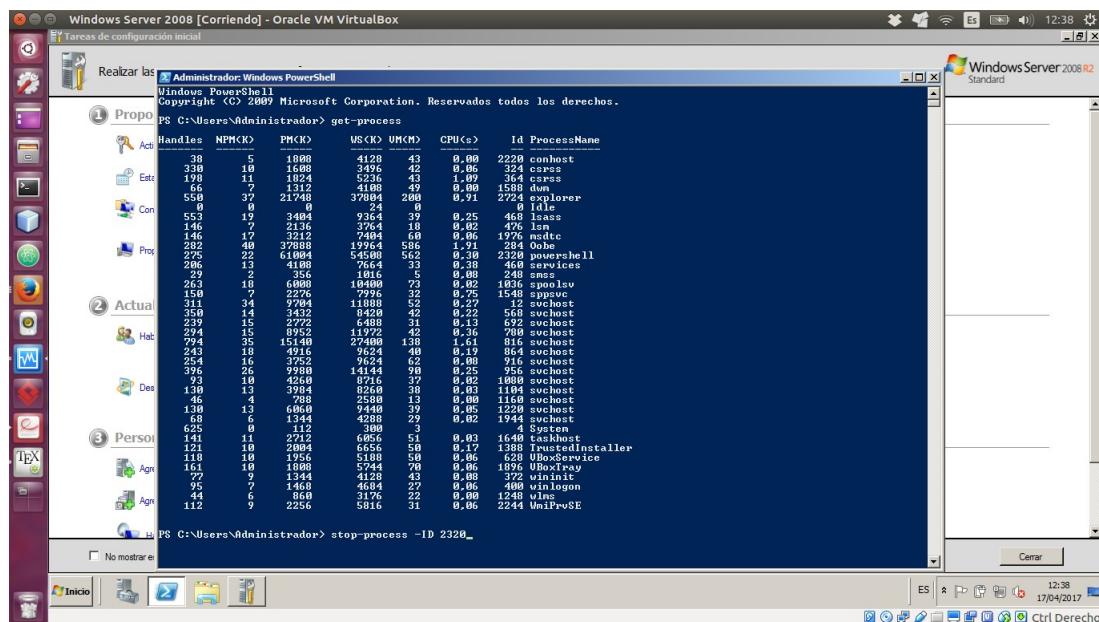


Figure 17.1: Parando el proceso powershell

Obviamente cuando ejecuto dicho comando lo que ocurre es que la consola de Powershell se cierra.

References

- [1] https://www.ssh.com/ssh/sshd_config/, year =.
- [2] Manual de ssh-copy-id: man ssh-copy-id, Consultado 10 de Abril del 2017.
- [3] <http://www.webmin.com/deb.html>, Consultado 14 de Abril del 2017.
- [4] <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-ssh-configfiles.html>, Consultado 14 de Abril del 2017.
- [5] <http://docs.python-guide.org/en/latest/starting/install3/linux/>, Consultado 17 de Abril del 2017.
- [6] https://docs.fedoraproject.org/es-ES/Fedora_Core/4/html/Software_Management_Guide/sn-yum-proxy-server.html, Consultado 17 de Abril del 2017.
- [7] <https://serverfault.com/questions/472605/how-do-do-this-in-apt-conf-acquirehttpproxy-1>, Consultado 17 de Abril del 2017.
- [8] <http://manpages.ubuntu.com/manpages/precise/man8/ufw.8.html>, Consultado 8 de Abril del 2017.
- [9] <http://manpages.ubuntu.com/manpages/wily/man1/add-apt-repository.1.html>, Consultado 8 de Abril del 2017.
- [10] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/s1-yum-useful-commands.html, Consultado 8 de Abril del 2017.
- [11] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sec-Managing_Yum_Repositories.html, Consultado 8 de Abril del 2017.
- [12] Manual de ssh-keygen: man ssh-keygen, Consultado el 10 de Abril del 2017.
- [13] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/sect-Managing_Services_with_systemd-Services.html, Consultado el 14 de Abril del 2017.
- [14] <https://wiki.debian.org/SSH>, Consultado el 14 de Abril del 2017.

[15] <http://php.net/manual/es/configuration.file.php>, Consultado el 17 de Abril del 2017.

[16] <http://fedoraproject.org/wiki/VMWare>, Consultado el 17 de Abril del 2017.

[17] <http://www.ssh.com/ssh/telnet>, Consultado el 8 de Abril del 2017.