

INGENIERÍA DE SERVIDORES (2016-2017)
SUBGRUPO A1
GRADO EN INGENIERÍA INFORMÁTICA
UNIVERSIDAD DE GRANADA

Práctica 2: Instalación y configuración de servicios

Mario Rodríguez Ruiz

24 de noviembre de 2016

Índice

1	Cuestión 1	7
1.1	Liste los argumentos de yum necesarios para instalar, buscar y eliminar paquetes	7
1.2	¿Qué ha de hacer para que yum pueda tener acceso a Internet en el PC del aula?(Pistas: archivo de configuración en /etc, proxy: stargate.ugr.es:3128)	8
1.3	¿Cómo añadimos un nuevo repositorio?	8
2	Cuestión 2	9
2.1	Liste los argumentos de apt necesarios para instalar, buscar y eliminar paquetes.	9
2.2	¿Qué ha de hacer para que apt pueda tener acceso a Internet en el PC del aula?(Pistas: archivo de configuración en /etc, proxy:stargate.ugr.es:3128)	10
2.3	¿Cómo añadimos un nuevo repositorio?	11
3	Cuestión 3	12
3.1	¿Con qué comando puede abrir/cerrar un puerto usando ufw? Muestre un ejemplo de cómo lo ha hecho	12
3.2	¿Con qué comando puede abrir/cerrar un puerto usando firewall-cmd en CentOS? Muestre un ejemplo de cómo lo ha hecho	13
3.3	Utilice el comando nmap para ver que, efectivamente, los puertos están accesibles	14
4	Cuestión 4	15
4.1	¿Qué diferencia hay entre telnet y ssh?	15
5	Cuestión 5	15
5.1	¿Para qué sirve la opción -X?	15
5.2	Ejecute remotamente, es decir, desde la máquina anfitriona (si tiene Linux) o desde la otra máquina virtual, el comando gedit en una sesión abierta con ssh. ¿Qué ocurre?	15
6	Cuestión 6	17
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. (Pistas: ssh-keygen, ssh-copyid).	17
7	Cuestión 7	20
7.1	¿Qué archivo es el que contiene la configuración del servicio ssh?	20
7.2	¿Qué parámetro hay que modificar para evitar que el usuario root acceda?	20
7.3	Cambie el puerto por defecto y compruebe que puede acceder	21

8 Cuestión 8	22
8.1 Indique si es necesario reiniciar el servicio ¿Cómo se reinicia un servicio en Ubuntu?	22
8.2 ¿y en CentOS? Muestre la secuencia de comandos para hacerlo.	22
9 Cuestión 9	23
9.1 Ubuntu Server: Instalación de Apache + MySQL + PHP	23
9.2 CentOS: Instalación de Apache + MySQL + PHP	23
9.2.1 Instalación MySQL / MariaDB	23
9.2.2 Instalación de Apache2	24
9.2.3 Instalación de PHP5	25
10 Cuestión 10	26
10.1 Realice la instalación usando GUI o PowerShell	26
10.2 Compruebe que el servicio está funcionando accediendo a la MV a través de la anfitriona	27
11 Cuestión 11	28
11.1 Muestre un ejemplo de uso del comando (p.ej. http://fedoraproject.org/wiki/VMWare)	28
12 Cuestión 12	29
12.1 Instalación de Webmin en CentOS	29
12.2 Ejecución de Webmin en CentOS	30
12.3 Apertura de puertos en CentOS desde Webmin	31
13 Cuestión 13	32
13.1 Instalación de phpMyAdmin en CentOS	32
13.2 Configuración de PHP para importar BDs de hasta 25MiB	34
14 Cuestión 14	37
15 Cuestión 15	41
15.1 Ejecute los ejemplos de find, grep	41
15.2 Escriba el script que haga uso de sed para cambiar la configuración de ssh y reiniciar el servicio.	41
15.3 Muestre un ejemplo de uso para awk	42
16 Cuestión 16	43
16.1 Escriba el script para cambiar el acceso a ssh usando PHP o Python. . . .	43
17 Cuestión 17	45
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.	45
18 Cuestión opcional 2	47

19 Cuestión opcional 3	49
20 Cuestión opcional 5	52
20.1 Realice la instalación de MongoDB en alguna de sus máquinas virtuales. . .	52
20.2 Cree una colección de documentos y haga una consulta sobre ellos. . . .	53

Índice de figuras

1.1. Instalación del paquete epel-release	7
1.2. Búsqueda del paquete kernel-devel	7
1.3. Borrado del paquete kernel-headers	8
1.4. Añadido del repositorio kde.repo	8
2.1. Instalación del paquete gcc	9
2.2. Búsqueda del paquete gedit	9
2.3. Borrado del paquete gedit	10
2.4. Añadido del repositorio shutter	11
3.1. Apertura del puerto 22 (SSH) con ufw	12
3.2. Denegado el acceso a través del puerto 22 (SSH) con ufw	13
3.3. Apertura del puerto 22 (SSH) con firewall-cmd	13
3.4. Denegado el acceso a través del puerto 22 (SSH) con firewall-cmd	14
3.5. Muestra de los puertos accesibles con nmap	14
5.1. Muestra información de las interfaces de la máquina de CentOS	15
5.2. Ejecución remota de gedit desde la máquina Ubuntu S.	16
5.3. Muestra información de las interfaces de la máquina de Ubuntu S.	16
5.4. Ejecución remota de gedit desde la máquina CentOS	16
6.1. Creación de las claves RSA	17
6.2. Copia de la clave en el host destino	18
6.3. Contenido de la clave pública de Centos	18
6.4. Clave de la máquina Centos dentro de Ubuntu	18
6.5. Conexión por ssh sin introducir contraseña	19
7.1. Fichero de configuración de ssh	20
7.2. Conexión por ssh sin introducir contraseña	20
7.3. Cambio del puerto SSH a 2222 en Centos	21
7.4. Conexión de Ubuntu a Centos con nuevo puerto ssh	21
8.1. Reinicio del servicio ssh en Ubuntu	22
8.2. Reinicio del servicio ssh en CentOS	22
9.1. Instalación de MySQL / MariaDB	23
9.2. Configuración de la cuenta root de MySQL	23
9.3. Instalación de Apache2	24
9.4. Configuración de arranque y apertura de puertos Apache	24
9.5. Prueba de Apache en el navegador	24
9.6. Instalación de PHP5	25
9.7. Creación de un fichero PHP5	25

9.8. Prueba de PHP5 en el navegador	25
10.1. Proceso de instalación del IIS en Windows Server	26
10.2. Prueba del servidor web en Windows Server	26
10.3. Prueba del servidor web (MV) desde la anfitriona	27
12.1. Creación de /etc/yum.repos.d/webmin.repo	29
12.2. Instalación de la clave GPG Webmin y de la herramienta.	29
12.3. Inicio, automatización del servicio y apertura del puerto necesario para Webmin	29
12.4. Inicio de Webmin a través del navegador.	30
12.5. Información del sistema desde Webmin	30
12.6. Puertos abiertos en el sistema	31
12.7. Apertura del puerto de telnet desde Webmin	31
13.1. Orden para la instalación de phpMyAdmin en CentOS	32
13.2. Cambio de la IP para acceder de forma remota a phpMyAdmin	33
13.3. Inicio y autenticación en phpMyAdmin	33
13.4. Pantalla principal de phpMyAdmin	34
13.5. Tamaño máximo inicial de archivos a importar en phpMyAdmin	34
13.6. Fichero de configuración de phpMyAdmin	35
13.7. Tamaño máximo actualizado de archivos a importar en phpMyAdmin	36
14.1. Página principal de ipsconfig	37
14.2. Login para administrador online demo en ipsconfig	38
14.3. Página principal de la demo de administrador de ipsconfig	38
14.4. Añadir un cliente en la demo de ipsconfig	39
14.5. Lista de clientes actualizada en la demo de ipsconfig	39
14.6. Estado del servidor en la demo online de ipsconfig	40
14.7. Cambio de idioma de la demo de ipsconfig	40
14.8. Cambio de idioma realizado de la demo de ipsconfig	40
15.1. Prueba de ejecución de find y grep	41
15.2. Script que cambia el puerto de ssh	42
15.3. Script en Bash que cambia el puerto de ssh	42
16.1. Script en Python que cambia el puerto de ssh	44
17.1. Información de los procesos en ejecución desde PowerShell	45
17.2. Parada de procesos desde PowerShell	46
18.1. Fichero de configuración /etc/fail2ban/jail.local	47
18.2. Archivo jail de protección SSH	47
18.3. Prueba de funcionamiento con fuerza bruta	48
18.4. Prueba de funcionamiento con fuerza bruta	48
19.1. Instalación del servicio RKhunter en Ubuntu Server	49
19.2. Configuración Postfix en Rhunter	49
19.3. Actualización de la base de datos de Rhunter	50
19.4. Primera ejecución de Rhunter	50
19.5. Advertencias en la ejecución Rhunter	51
19.6. Resultados de la ejecución de Rhunter	51
20.1. Fichero de configuración del repositorio de MongoDB	52

20.2. Instalación de MongoDB en Centos 7	52
20.3. Guardado de una colección en Mongo	54
20.4. Consulta de documentos de una colección en Mongo	54

1. Cuestión 1

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

Argumentos de yum[2]:

- Para instalar: > **sudo yum install *paquete***

En la Figura 1.1 se muestra la instalación el paquete **epel-release** desde Centos 7.

```
MRR jue nov 17> sudo yum install epel-release
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.xtratelecom.es
 * extras: centos.mirror.xtratelecom.es
 * updates: centos.mirror.xtratelecom.es
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete epel-release.noarch 0:7-6 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

=====
Package                Arquitectura  Versión      Repositorio
=====
Instalando:
epel-release            noarch       7-6          extras

Resumen de la transacción
=====
Instalar 1 Paquete

Tamaño total de la descarga: 14 k
Tamaño instalado: 24 k
Is this ok [y/d/N]: y
```

Figura 1.1: Instalación del paquete **epel-release**

- Para buscar: > **yum search *paquete***

En la Figura 1.2 se muestra la búsqueda del paquete **kernel-devel** desde Centos 7.

```
MRR jue nov 17> yum search kernel-devel
Complementos cargados:fastestmirror, langpacks
Determining fastest mirrors
 * base: centos.cadt.com
 * epel: epel.besthosting.ua
 * extras: centos.cadt.com
 * updates: centos.cadt.com
===== N/S matched: kernel-devel =====
kernel-devel.x86_64 : Development package for building kernel modules to match
                     : the kernel

Nombre y resumen que coinciden con y sólo , use "buscar todo" para todo.
MRR jue nov 17> █
```

Figura 1.2: Búsqueda del paquete **kernel-devel**

- Para borrar: `> sudo yum remove paquete`

En la Figura 1.3 se muestra cómo se borra el paquete **kernel-headers** desde Centos 7.

```
MRR jue nov 17> sudo yum remove kernel-headers
Complementos cargados:fastestmirror, langpacks
Resolviendo dependencias
--> Ejecutando prueba de transacción
--> Paquete kernel-headers.x86_64 0:3.10.0-327.36.3.el7 debe ser eliminado
--> Procesando dependencias: kernel-headers para el paquete: glibc-headers-2.17-106.el7_2.8.x86_64
--> Procesando dependencias: kernel-headers >= 2.2.1 para el paquete: glibc-headers-2.17-106.el7_2.8.x86_64
--> Ejecutando prueba de transacción
--> Paquete glibc-headers.x86_64 0:2.17-106.el7_2.8 debe ser eliminado
--> Procesando dependencias: glibc-headers para el paquete: glibc-devel-2.17-106.el7_2.8.x86_64
--> Procesando dependencias: glibc-headers = 2.17-106.el7_2.8 para el paquete: glibc-devel-2.17-106.el7_2.8.x86_64
--> Ejecutando prueba de transacción
--> Paquete glibc-devel.x86_64 0:2.17-106.el7_2.8 debe ser eliminado
--> Procesando dependencias: glibc-devel >= 2.2.90-12 para el paquete: gcc-4.8.5-4.el7.x86_64
--> Ejecutando prueba de transacción
--> Paquete gcc.x86_64 0:4.8.5-4.el7 debe ser eliminado
```

Figura 1.3: Borrado del paquete **kernel-headers**

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

Para que **yum** pueda tener acceso a Internet en el PC del aula hay que editar el fichero de configuración `/etc/yum.conf`^[15] añadiéndole una nueva línea que contendrá lo siguiente:

```
proxy=stargate.ugr.es:3128
```

1.3. ¿Cómo añadimos un nuevo repositorio?

Para añadir un nuevo repositorio se utiliza la herramienta **yum-config-manager**^[8] que permite, entre otras, dicha gestión. Un ejemplo de ejecución sería:

```
> yum-config-manager --add-repo=url
```

En la Figura 1.4 se muestra cómo se añade el repositorio **kde.repo** desde Centos 7.

```
MRR jue nov 17> sudo yum-config-manager --add-repo=http://apt.kde-redhat.org/apt/kde-redhat/fedora/kde.repo
Complementos cargados:fastestmirror, langpacks
adding repo from: http://apt.kde-redhat.org/apt/kde-redhat/fedora/kde.repo
grabbing file http://apt.kde-redhat.org/apt/kde-redhat/fedora/kde.repo to /etc/yum.repos.d/kde.repo
kde.repo | 799 B 00:00
repo saved to /etc/yum.repos.d/kde.repo
MRR jue nov 17>
```

Figura 1.4: Añadido del repositorio **kde.repo**

2. Cuestión 2

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

Argumentos de apt[28]:

- Para instalar: `> sudo apt-get install paquete`[28]

En la Figura 2.1 se muestra cómo se instala el paquete `gcc` en Ubuntu Server.

```
MRR jue nov 17> sudo apt-get install gcc
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  binutils cpp cpp-5 gcc-5 libasan2 libatomic1 libc-dev-bin libc6 libc6-dev libcc1-0 libcilkrts5
  libgcc-5-dev libgomp1 libisl15 libitm1 liblsan0 libmpc3 libmpx0 libquadmath0 libtsan0 libubsan0
  linux-libc-dev manpages-dev
Paquetes sugeridos:
  binutils-doc cpp-doc gcc-5-locales gcc-multilib make autoconf automake libtool flex bison gdb
  gcc-doc gcc-5-multilib gcc-5-doc libgcc1-dbg libgomp1-dbg libitm1-dbg libatomic1-dbg
  libasan2-dbg liblsan0-dbg libtsan0-dbg libubsan0-dbg libcilkrts5-dbg libmpx0-dbg
  libquadmath0-dbg glibc-doc
Se instalarán los siguientes paquetes NUEVOS:
  binutils cpp cpp-5 gcc gcc-5 libasan2 libatomic1 libc-dev-bin libc6-dev libcc1-0 libcilkrts5
  libgcc-5-dev libgomp1 libisl15 libitm1 liblsan0 libmpc3 libmpx0 libquadmath0 libtsan0 libubsan0
  linux-libc-dev manpages-dev
Se actualizarán los siguientes paquetes:
  libc6
1 actualizados, 23 nuevos se instalarán, 0 para eliminar y 66 no actualizados.
4 no instalados del todo o eliminados.
Se necesita descargar 30,0 MB de archivos.
Se utilizarán 99,6 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Figura 2.1: Instalación del paquete `gcc`

- Para buscar: `> apt-cache search paquete`[28]

En la Figura 2.2 se muestra cómo se busca el paquete `gedit` en Ubuntu Server.

```
MRR jue nov 17> apt-cache search gedit
gedit - Editor de texto oficial del entorno de escritorio GNOME
gedit-common - Editor de texto oficial del entorno de escritorio GNOME (archi
gedit-dev - Editor de texto oficial para el entorno del escritorio de GNOME
gedit-plugins - conjunto de complementos para gedit
gigedit - Editor de instrumentos para archivos Gigasampler
leafpad - Editor de texto simple basado en GTK+
libgtk2-sourceview2-perl - enhanced source code editor widget
libwin-hivex-perl - Vínculos Perl para hivex
rabbitvcs-gedit - Extensión de Gedit para RabbitVCS
debugedit - tool to mangle source locations in .debug files
```

Figura 2.2: Búsqueda del paquete `gedit`

- Para borrar: `> sudo apt remove paquete`[\[28\]](#)

En la Figura 2.3 se muestra cómo se borra el paquete **gedit** en Ubuntu Server.

```
MRR jue nov 17> sudo apt remove gedit
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
adwaita-icon-theme aspell aspell-en at-spi2-core colord colord-data dconf-gsettings-backend
dconf-service dictionaries-common enacsen-common enchant fontconfig fontconfig-config
fonts-dejavu-core gedit-common gir1.2-atk-1.0 gir1.2-freedesktop gir1.2-gdkpixbuf-2.0
gir1.2-gtk-3.0 gir1.2-gtksource-3.0 gir1.2-pango-1.0 gir1.2-peas-1.0 glib-networking
glib-networking-common glib-networking-services gnome-user-guide gsettings-desktop-schemas
gstreamer1.0-plugins-base gstreamer1.0-plugins-good gstreamer1.0-x hicolor-icon-theme
humanity-icon-theme hunspell-en-us libaa1 libaspell15 libatk-bridge2.0-0 libatk1.0-0
libatk1.0-data libatspi2.0-0 libavahi-client3 libavahi-common-data libavahi-common3 libavc1394-0
libboost-filesystem1.58.0 libboost-system1.58.0 libcaca0 libcairo-gobject2 libcairo2
libcdparanoia0 libcolord2 libcolorhug2 libcroc3 libcups2 libdatrie1 libdconf1 libdrm-amdgpu1
libdrm-intel1 libdrm-nouveau2 libdrm-radeon1 libdv4 libegl1-mesa libenchantic2a libepoxy0
libexif12 libflac8 libfontconfig1 libgbm1 libgd3 libgdk-pixbuf2.0-0 libgdk-pixbuf2.0-common
libgeoclue0 libgl1-mesa-dri libgl1-mesa-glx libglapi-mesa libgphoto2-6 libgphoto2-l10n
libgphoto2-port12 libgraphite2-3 libgstreamer-plugins-base1.0-0 libgstreamer-plugins-good1.0-0
libgstreamer1.0-0 libgtk-3-0 libgtk-3-bin libgtk-3-common libgtk2.0-0 libgtk2.0-bin
libgtk2.0-common libgtksourceview-3.0-1 libgtksourceview-3.0-common libgudev-1.0-0 libgusb2
```

Figura 2.3: Borrado del paquete **gedit**

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

Para que **apt** pueda tener acceso a Internet en el PC del aula existen tres métodos[\[25\]](#):

- Sesión de proxy temporal.

Este modo de acceso se debe configurar manualmente cada vez que desee utilizar apt-get a través de un proxy HTTP.

Para ello se debe de introducir la siguiente orden en un terminal:

```
> export http_proxy = http: // stargate.ugr.es: 3128
```

- Modificación del fichero de configuración de APT.

Editar el fichero de configuración `/etc/apt.conf`[\[13\]](#) añadiéndole una nueva linea que contendrá lo siguiente:

```
Acquire :: http :: Proxy "http: // stargate.ugr.es: 3128" ;
```

- Modificación del fichero de configuración de BASH[\[10\]](#).

Editar el fichero de configuración `~/.bashrc` añadiéndole dos nuevas lineas que contendrán lo siguiente:

```
http_proxy = http: // stargate.ugr.es: 3128
export http_proxy
```

2.3. ¿Cómo añadimos un nuevo repositorio?

Para añadir un nuevo repositorio se introduce la siguiente orden en un terminal[9, 26]:

```
> sudo add-apt-repository ppa:repositorio
```

Donde *repositorio* es el nombre del repositorio a añadir.



```
MRR vie nov 18> sudo add-apt-repository ppa:shutter/ppa
[sudo] password for mario:
This is the official Shutter repository - it is recommended to use this to keep your Shutter easily
updated.

For instructions on how to add the repository, see (http://shutter-project.org/faq-help/ppa-installat
ion-guide).
Más información: https://launchpad.net/~shutter/+archive/ubuntu/ppa
Pulse [Intro] para continuar o ctrl-c para cancelar
```

Figura 2.4: Añadido del repositorio **shutter**

En la Figura 2.4 se muestra cómo se añade el repositorio **shutter** en Ubuntu Server.

3. Cuestión 3

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

Comandos **ufw**[27]:

- Para abrir un puerto: > **sudo ufw allow *puerto***[27]

Al no tener activo el servicio, primero hay que activarlo y luego establecerle una configuración determinada: En este caso se ha denegado cualquier conexión entrante con la especificación **default deny**.

A continuación se reinicia el servicio, desactivándolo y activándolo de forma seguida.

Por último se abre el puerto 22.

En la Figura 3.1 se muestra todo el proceso descrito anteriormente.

```
MRR vie nov 18> sudo ufw status
Estado: inactivo
MRR vie nov 18> sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
MRR vie nov 18> sudo ufw default deny
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
MRR vie nov 18> sudo ufw disable
El cortafuegos está detenido y deshabilitado en el arranque del sistema
MRR vie nov 18> sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
MRR vie nov 18> sudo ufw allow 22
Regla añadida
Regla añadida (v6)
MRR vie nov 18>
```

Figura 3.1: Apertura del puerto 22 (SSH) con ufw

- Para cerrar un puerto: > **sudo ufw deny *puerto***[27]

En la Figura 3.2 se muestra en primer lugar el estado actual de los puertos. Aparece el como abierto el puerto 22, por lo que se procede a cerrarlo.

De nuevo se comprueba el estado de los puertos y se aprecia cómo ya esta cerrado.

```

MRR vie nov 18> sudo ufw status verbose
[sudo] password for mario:
Estado: activo
Acceso: on (low)
Predeterminado: deny (entrantes), allow (salientes), disabled (enrutados)
Perfiles nuevos: skip

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

MRR vie nov 18> sudo ufw deny 22
Regla actualizada
Regla actualizada (v6)
MRR vie nov 18> sudo ufw status verbose
Estado: activo
Acceso: on (low)
Predeterminado: deny (entrantes), allow (salientes), disabled (enrutados)
Perfiles nuevos: skip

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

```

Figura 3.2: Denegado el acceso a través del puerto **22** (SSH) con ufw

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

Comandos **firewall-cmd**:

- Para abrir un puerto: > **firewall-cmd --zone=zona --add-port=puerto/protocolo**[24, 22]

En la Figura 3.3 se muestra en primer lugar el la lista actual de los puertos abiertos. De forma seguida se abre el puerto 22/tcp.

```

MRR vie nov 18> sudo firewall-cmd --zone=dmz --list-port
MRR vie nov 18> sudo firewall-cmd --zone=dmz --add-port=22/tcp
success
MRR vie nov 18> sudo firewall-cmd --zone=dmz --list-port
22/tcp
MRR vie nov 18> █

```

Figura 3.3: Apertura del puerto **22** (SSH) con firewall-cmd

- Para cerrar un puerto: > **firewall-cmd --zone=zona --remove-port=puerto/protocolo**[24, 22]

En la Figura 3.4 se muestra en primer lugar el la lista actual de los puertos abiertos. De forma seguida se abre el puerto 22/tcp.

```

MRR vie nov 18> sudo firewall-cmd --zone=dmz --list-port
22/tcp
MRR vie nov 18> sudo firewall-cmd --zone=dmz --remove-port=22/tcp
success
MRR vie nov 18> sudo firewall-cmd --zone=dmz --list-port
MRR vie nov 18> █

```

Figura 3.4: Denegado el acceso a través del puerto **22** (SSH) con firewall-cmd

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

En la Figura 3.5 pueden verse los puertos que están accesibles mediante el comando **nmap** [16]. En primer lugar se muestran los accesibles desde el localhost y, en segundo lugar, los accesibles de una cualquier dirección al azar.

```

MRR vie nov 18> nmap localhost

Starting Nmap 6.40 ( http://nmap.org ) at 2016-11-18 16:48 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00098s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
631/tcp    open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
MRR vie nov 18> nmap 108.61.155.194

Starting Nmap 6.40 ( http://nmap.org ) at 2016-11-18 16:48 CET
Nmap scan report for my.serverbundle.com (108.61.155.194)
Host is up (0.49s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    closed https

Nmap done: 1 IP address (1 host up) scanned in 77.58 seconds
MRR vie nov 18> █

```

Figura 3.5: Muestra de los puertos accesibles con **nmap**

4. Cuestión 4

4.1. ¿Qué diferencia hay entre telnet y ssh?

La diferencia más contundente que existe entre telnet y ssh es que **en ssh el tráfico se encuentra cifrado** y en telnet no. Esto es por el uso que realiza SSH con claves criptográficas públicas y privadas. El par de claves SSH son generadas con algoritmos como RSA y DSA aunque ECDSA es el que recomienda OpenSSH por ofrecer la misma seguridad con un menor tamaño en bits para las claves.

Otras diferencias son, por ejemplo, que funcionan en puertos diferentes: **telnet utiliza el puerto 23** mientras que ssh el 22 y que telnet usa un poco menos de sobrecarga de ancho de banda en comparación con ssh.

[4, 3]

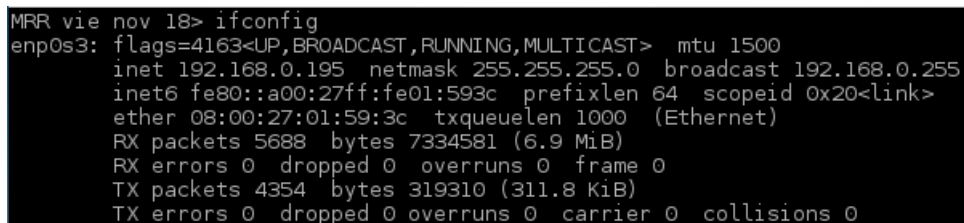
5. Cuestión 5

5.1. ¿Para qué sirve la opción -X?

La opción -X [17] sirve para habilitar el **X11 forwarding**. Éste permite que la aplicación gráfica se ejecute en el servidor y se exporte el display a la máquina cliente. Es decir, la aplicación simulará ejecutarse en la máquina anfitriona pero en realidad se estará ejecutando en el servidor.

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

En primer lugar se va a realizar una conexión desde la máquina de Ubuntu a la de Centos. En la Figura 5.1 se muestra cuál es la dirección de la máquina de Centos para poder conectarse con ella.



```
MRR vie nov 18> ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.195 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe01:593c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:01:59:3c txqueuelen 1000 (Ethernet)
    RX packets 5688 bytes 7334581 (6.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4354 bytes 319310 (311.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 5.1: Muestra información de las interfaces de la máquina de CentOS

La Figura 5.2 muestra la conexión entre las máquinas y, además, cómo no es posible la apertura gráfica de gedit, ya que este sistema operativo no dispone de interfaz gráfica de ventanas.

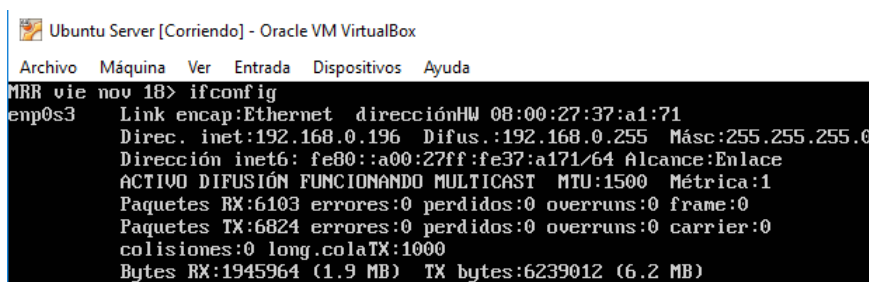
```

MRR vie nov 18> ssh -X mario@192.168.0.195
The authenticity of host '192.168.0.195 (192.168.0.195)' can't be established.
ECDSA key fingerprint is SHA256:b4ELfcXc4lwPhpExRduYXCfaB+Rwe1heyI5aXu6T03I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.195' (ECDSA) to the list of known hosts.
mario@192.168.0.195's password:
Last login: Fri Nov 18 17:17:07 2016
[mario@localhost ~]$ gedit &
[1] 4670
[mario@localhost ~]$
(gedit:4670): Gtk-WARNING **: cannot open display:

```

Figura 5.2: Ejecución remota de gedit desde la máquina Ubuntu S.

Sin embargo, si la conexión se realiza de manera inversa (desde Ubuntu hacia Centos y siempre utilizando la opción -X en estos casos), no existe ningún problema. Véase en las Figuras 5.3 y 5.4 en las que se prueba dicha ejecución.



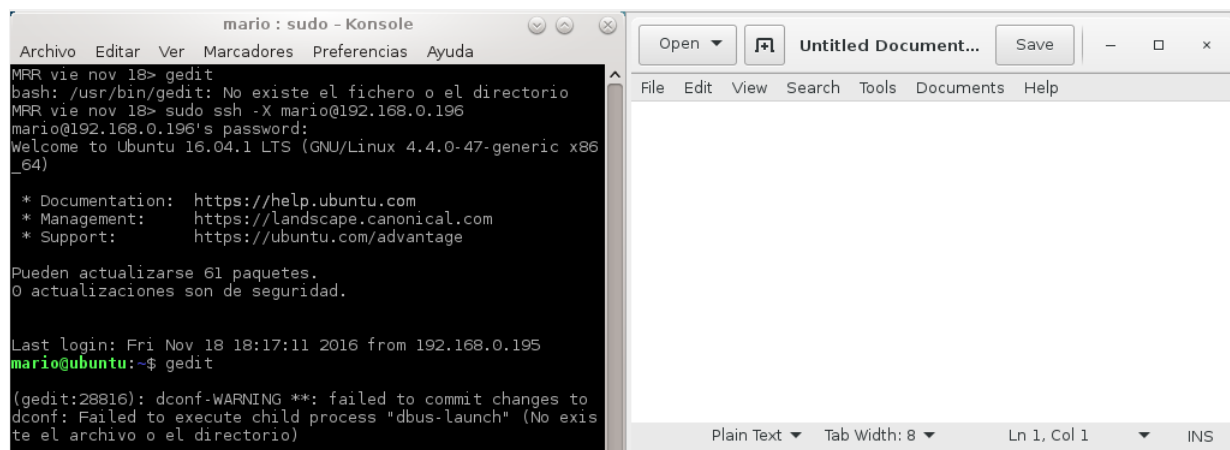
```

Ubuntu Server [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
MRR vie nov 18> ifconfig
enp0s3    Link encap:Ethernet  direcciónHW 08:00:27:37:a1:71
          Direc. inet:192.168.0.196  Difus.:192.168.0.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe37:a171/64  Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:6103 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:6824 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colatX:1000
          Bytes RX:1945964 (1.9 MB)  TX bytes:6239012 (6.2 MB)

```

Figura 5.3: Muestra información de las interfaces de la máquina de Ubuntu S.

La Figura 5.3 muestra la dirección de la máquina Ubuntu para poder realizar la conexión sobre ella.



```

mario : sudo - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
MRR vie nov 18> gedit
bash: /usr/bin/gedit: No existe el fichero o el directorio
MRR vie nov 18> sudo ssh -X mario@192.168.0.196
mario@192.168.0.196's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Pueden actualizarse 61 paquetes.
0 actualizaciones son de seguridad.

Last login: Fri Nov 18 18:17:11 2016 from 192.168.0.195
mario@ubuntu:~$ gedit
(gedit:28816): dconf-WARNING **: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No existe el archivo o el directorio)

```

Figura 5.4: Ejecución remota de gedit desde la máquina CentOS

Como se ve en la Figura 5.4 gedit no se encuentra instalado en la máquina CentOS, por lo que se prueba que la ejecución se realiza en la máquina Ubuntu S.

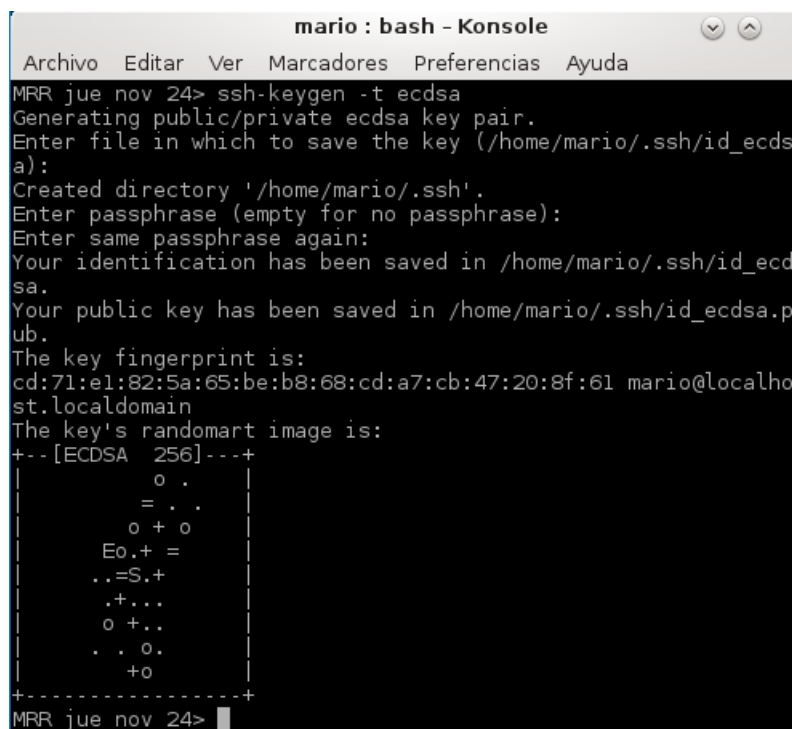
6. Cuestión 6

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. (Pistas: `ssh-keygen`, `ssh-copyid`).

En primer lugar se generan las claves RSA en el host desde el que va a realizar la conexión (CentOS, en este caso) a través del comando:

```
> ssh-keygen -t rsa [12]
```

La Figura 6.1 muestra la creación de las claves ECDSA para su posterior utilización en SSH.



```
mario : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR jue nov 24> ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/mario/.ssh/id_ecdsa):
Created directory '/home/mario/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/mario/.ssh/id_ecdsa.
Your public key has been saved in /home/mario/.ssh/id_ecdsa.pub.
The key fingerprint is:
cd:71:e1:82:5a:65:be:b8:68:cd:a7:cb:47:20:8f:61 mario@localhost.localdomain
The key's randomart image is:
+--[ECDSA 256]--+
|                 |
|      o  .       |
|      = . .      |
|    o + o        |
|   Eo.+ =        |
|  ..=S.+         |
| .+. . .         |
| o + ..          |
| . . o.          |
|   +o            |
+-----+
MRR jue nov 24> █
```

Figura 6.1: Creación de las claves RSA

A continuación, desde el mismo host (CentOS), se copiará la clave generada anteriormente en el host al que se quiere conectar (Ubuntu S.) por medio de la orden [11]:

```
> ssh-copy-id usuario@ip
```

La Figura 6.2 muestra cómo se copian las claves en el host destino a través de su IP.

```
MRR jue nov 24> ssh-copy-id mario@192.168.1.38
The authenticity of host '192.168.1.38 (192.168.1.38)' can't
be established.
ECDSA key fingerprint is 61:5a:bf:a3:db:74:f1:83:8a:af:7a:6e:
1e:df:6c:17.
Are you sure you want to continue connecting (yes/no)? yes
/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 prompted now it is to install the new keys
mario@192.168.1.38's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'mario@192.168
.1.38'"
and check to make sure that only the key(s) you wanted were a
dded.

MRR jue nov 24> █
```

Figura 6.2: Copia de la clave en el host destino

La clave publica generada en la máquina Centos, Figura 6.3, es la que se encuentra en `~/ssh/id_ecdsa.pub` y que se ha enviado a la máquina Ubuntu.

```
mario : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR jue nov 24> cat .ssh/
id_ecdsa      id_ecdsa.pub  known_hosts
MRR jue nov 24> cat .ssh/id_ecdsa.pub
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzd
HAyNTYAAABBBNPwa4Y6t7IjbZizhlw1jKY8mEzKpj/4S0DFQJQpHC60Wat2V1
GwlyIvUHjedgq9lU8vatxh2AAGBD111HHI5PA= mario@localhost.locald
omain
MRR jue nov 24> █
```

Figura 6.3: Contenido de la clave pública de Centos

Se puede comprobar ahora en la máquina Ubuntu en el fichero `~/ssh/authorized_keys` cómo se encuentra la misma clave anterior. La Figura 6.4 muestra el contenido del fichero mencionado de Ubuntu.

```
MRR jue nov 24> cat .ssh/authorized_keys
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNPwa4Y6t7IjbZizhlw1jKY8mEzK
pj/4S0DFQJQpHC60Wat2V1GwlyIvUHjedgq9lU8vatxh2AAGBD111HHI5PA= mario@localhost.localdomain
MRR jue nov 24> █
```

Figura 6.4: Clave de la máquina Centos dentro de Ubuntu

En la Figura 6.2 se ve cómo se ha requerido la contraseña de administrador de Ubuntu para conectarse desde Centos. Pues bien, esta ha sido la última vez que sucederá. Prueba de ello existe en la Figura 6.5

```
MRR vie nov 18> ssh -X mario@192.168.0.196
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Pueden actualizarse 61 paquetes.
0 actualizaciones son de seguridad.

Last login: Fri Nov 18 18:18:47 2016 from 192.168.0.195
mario@ubuntu:~$
```

Figura 6.5: Conexión por ssh sin introducir contraseña

7. Cuestión 7

7.1. ¿Qué archivo es el que contiene la configuración del servicio ssh?

El archivo que contiene la configuración del servicio ssh es `/etc/ssh/sshd_config` [14]. Parte de su contenido puede verse en la Figura 7.1

```
MRR jue nov 24> cat /etc/ssh/sshd_config
#
# $OpenBSD: ssh_config,v 1.28 2013/09/16 11:35:43 sthen
# Exp $
#
# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides def
# aults for
# users, and the values can be changed in per-user configurat
# ion 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 i
# s 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 c
# omprehensive
# list of available options, their meanings and defaults, ple
# ase see the
# ssh_config(5) man page.
```

Figura 7.1: Fichero de configuración de ssh

7.2. ¿Qué parámetro hay que modificar para evitar que el usuario root acceda?

El parámetro que hay que modificar para evitar que el usuario root acceda es *PermitRootLogin*, su posición en el fichero puede verse en la Figura 7.2

```
GNU nano 2.3.1 Fichero: /etc/ssh/sshd_config
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

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

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Figura 7.2: Conexión por ssh sin introducir contraseña

La modificación debe quedar así en el fichero:

PermitRootLogin no

7.3. Cambie el puerto por defecto y compruebe que puede acceder

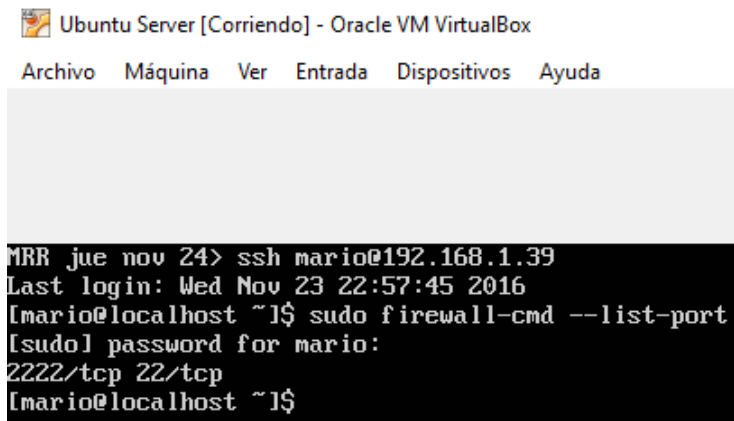
Para cambiar el puerto por defecto hay que modificar el valor de **Port** dentro del fichero `/etc/ssh/sshd_config`.

En ese fichero se ha cambiado su valor por el de 2222. La Figura 7.3 muestra que se ha cambiado dicho valor a través de nano, a continuación se ha abierto el puerto nuevo y por último, por `ipconfig` aparece la IP de Centos que va a utilizar la máquina de Ubuntu para conectarse por ssh.

```
MRR jue nov 24> sudo nano /etc/ssh/sshd_config
MRR jue nov 24> sudo firewall-cmd --list-port
22/tcp
MRR jue nov 24> sudo firewall-cmd --add-port=2222/tcp
success
MRR jue nov 24> sudo firewall-cmd --list-port
2222/tcp 22/tcp
MRR jue nov 24> ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.39 netmask 255.255.255.0 broadcast 1
    92.168.1.255
    inet6 fd4b:bb6e:df59:0:a00:27ff:fe01:593c prefixlen
    64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:fe01:593c prefixlen 64 scopeid
    0x20<link>
```

Figura 7.3: Cambio del puerto SSH a **2222** en Centos

En la Figura 7.4 puede demostrarse que no ha habido ningún problema con el acceso después de hacer el cambio del valor del puerto.



```

MRR jue nov 24> ssh mario@192.168.1.39
Last login: Wed Nov 23 22:57:45 2016
[mario@localhost ~]$ sudo firewall-cmd --list-port
[sudo] password for mario:
2222/tcp 22/tcp
[mario@localhost ~]$
```

Figura 7.4: Conexión de Ubuntu a Centos con nuevo puerto ssh

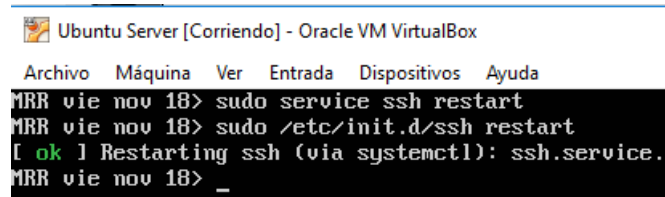
8. Cuestión 8

8.1. Indique si es necesario reiniciar el servicio ¿Cómo se reinicia un servicio en Ubuntu?

Es necesario reiniciar el servicio si se quiere que los cambios sean válidos en ese momento. De no ser así hay que esperar a un reinicio del sistema operativo para que los cambios realizados surjan efecto.

Para reiniciar el servicio en Ubuntu existen dos métodos distintos [18]:

- > `sudo service servicio restart`
- > `sudo /etc/init.d/servicio restart`

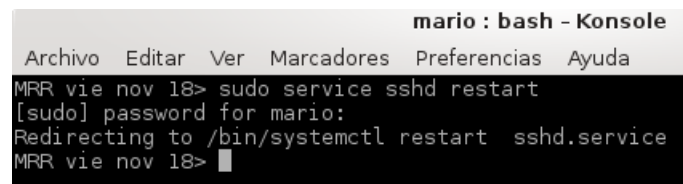


```
Ubuntu Server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
MRR vie nov 18> sudo service ssh restart
MRR vie nov 18> sudo /etc/init.d/ssh restart
[ ok ] Restarting ssh (via systemctl): ssh.service.
MRR vie nov 18> _
```

Figura 8.1: Reinicio del servicio **ssh** en Ubuntu

8.2. ¿y en CentOS? Muestre la secuencia de comandos para hacerlo.

- > `sudo service servicio restart` [1]



```
mario : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR vie nov 18> sudo service sshd restart
[sudo] password for mario:
Redirecting to /bin/systemctl restart  sshd.service
MRR vie nov 18> █
```

Figura 8.2: Reinicio del servicio **ssh** en CentOS

9. Cuestión 9

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.

9.1. Ubuntu Server: Instalación de Apache + MySQL + PHP

[6]

```
> sudo apt-get install lamp-server^
```

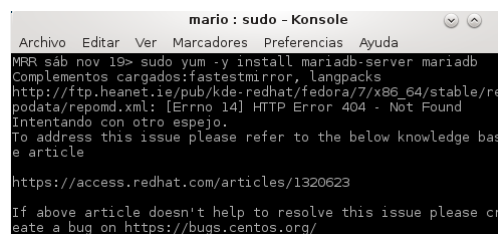
```
> sudo service apache2 restart
```

9.2. CentOS: Instalación de Apache + MySQL + PHP

[31]

9.2.1. Instalación MySQL / MariaDB

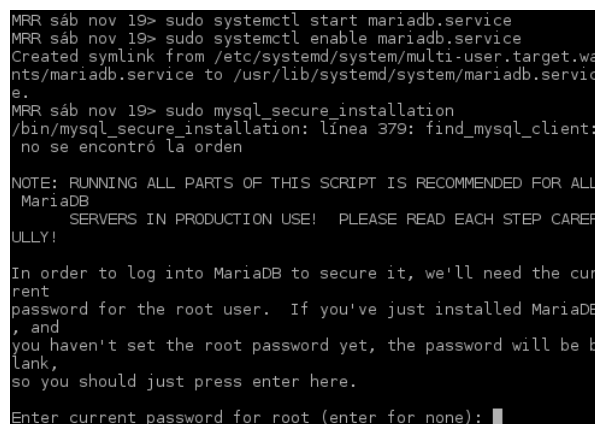
- Orden para la instalación a través de la línea de comandos, Figura 9.1:



```
mario : sudo - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
MRR sáb nov 19> sudo yum -y install mariadb-server mariadb
Complementos cargados:fastestmirror, langpacks
http://ftp.heanet.ie/pub/kde-redhat/fedora/7/x86_64/stable/re
podata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Intentando con otro espejo.
To address this issue please refer to the below knowledge bas
e article
https://access.redhat.com/articles/1320623
If above article doesn't help to resolve this issue please cr
eate a bug on https://bugs.centos.org/
```

Figura 9.1: Instalación de MySQL / MariaDB

- Configuración de arranque inicial en el sistema y de la cuenta root, Figura 9.2:



```
MRR sáb nov 19> sudo systemctl start mariadb.service
MRR sáb nov 19> sudo systemctl enable mariadb.service
Created symlink from /etc/systemd/system/multi-user.target.wa
nts/mariadb.service to /usr/lib/systemd/system/mariadb.servic
e.
MRR sáb nov 19> sudo mysql_secure_installation
/bin/mysql_secure_installation: línea 379: find_mysql_client:
no se encontró la orden

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL
MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREF
ULLY!

In order to log into MariaDB to secure it, we'll need the cur
rent
password for the root user. If you've just installed MariaDB
, and
you haven't set the root password yet, the password will be b
lank,
so you should just press enter here.

Enter current password for root (enter for none):
```

Figura 9.2: Configuración de la cuenta root de MySQL

9.2.2. Instalación de Apache2

- Orden para la instalación a través de la línea de comandos, Figura 9.3:

```
MRR sáb nov 19> sudo yum -y install httpd
[sudo] password for mario:
Complementos cargados:fastestmirror, langpacks
http://ftp.heanet.ie/pub/kde-redhat/fedora/7/x86_64/stable/re
podata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Intentando con otro espejo.
To address this issue please refer to the below knowledge bas
e article
https://access.redhat.com/articles/1320623
If above article doesn't help to resolve this issue please cr
eate a bug on https://bugs.centos.org/
```

Figura 9.3: Instalación de Apache2

- Configuración de arranque inicial en el sistema y apertura de los puertos necesarios, Figura 9.4:

```
MRR sáb nov 19> sudo systemctl start httpd.service
MRR sáb nov 19> sudo systemctl enable httpd.service
Created symlink from /etc/systemd/system/multi-user.target.wa
nts/httpd.service to /usr/lib/systemd/system/httpd.service.
MRR sáb nov 19> sudo firewall-cmd --permanent --zone=public --
-add-service=http
success
MRR sáb nov 19> sudo firewall-cmd --permanent --zone=public --add-
service=https
success
MRR sáb nov 19> sudo firewall-cmd --reload
success
MRR sáb nov 19> █
```

Figura 9.4: Configuración de arranque y apertura de puertos Apache

- Prueba del funcionamiento desde el navegador, Figura 9.5:

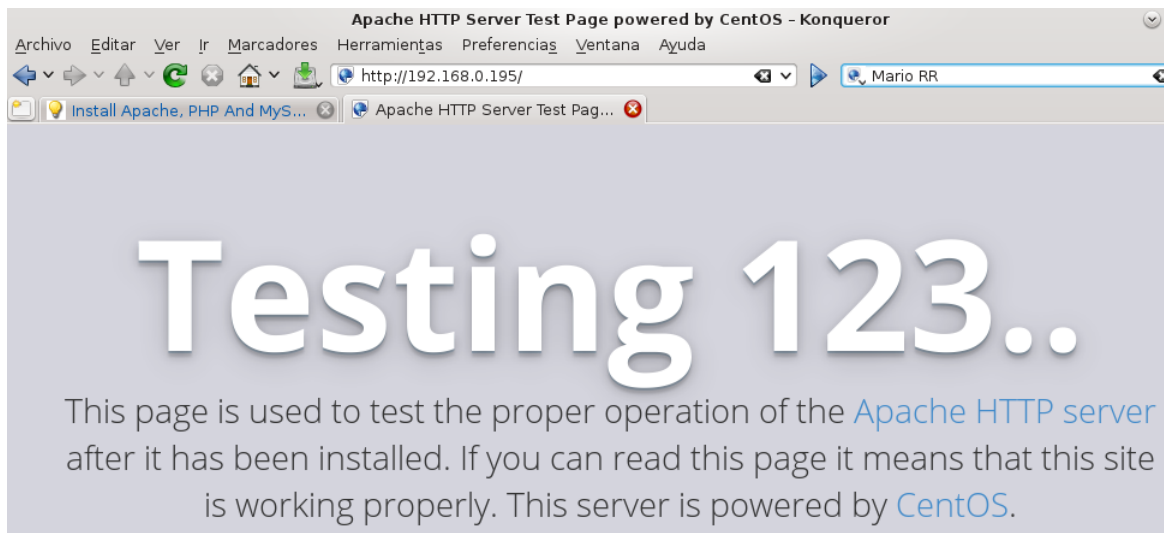


Figura 9.5: Prueba de Apache en el navegador

9.2.3. Instalación de PHP5

- Orden para la instalación a través de la línea de comandos, Figura 9.6:

```
MRR sáb nov 19> sudo yum -y install php
[sudo] password for mario:
Complementos cargados:fastestmirror, langpacks
http://ftp.heanet.ie/pub/kde-redhat/fedora/7/x86_64/stable/re
podata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Intentando con otro espejo.
To address this issue please refer to the below knowledge bas
e article
https://access.redhat.com/articles/1320623
If above article doesn't help to resolve this issue please cr
eate a bug on https://bugs.centos.org/
```

Figura 9.6: Instalación de PHP5

- Creación de un fichero PHP5 para su posterior prueba, Figura 9.7:

```
mario : sudo - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
GNU nano 2.3.1 Fichero: ...r/www/html/info.php
?php
phpinfo();
?>
```

Figura 9.7: Creación de un fichero PHP5

- Prueba del funcionamiento desde el navegador, Figura 9.8:

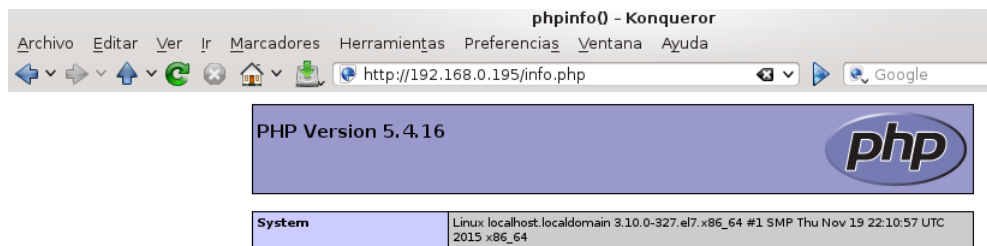


Figura 9.8: Prueba de PHP5 en el navegador

10. Cuestión 10

10.1. Realice la instalación usando GUI o PowerShell

Se ha realizado la instalación usando GUI [31]. El proceso de instalación realizado usando el asistente para agregar roles y características puede verse en la Figura 10.1:

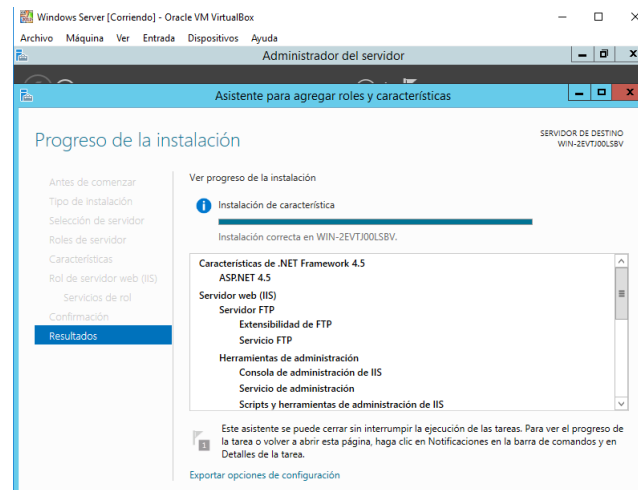


Figura 10.1: Proceso de instalación del IIS en Windows Server

Una vez terminada la instalación puede comprobarse que el servicio funciona a través del navegador web, poniendo en la barra de direcciones **http://localhost/**, como se hace en la Figura 10.2

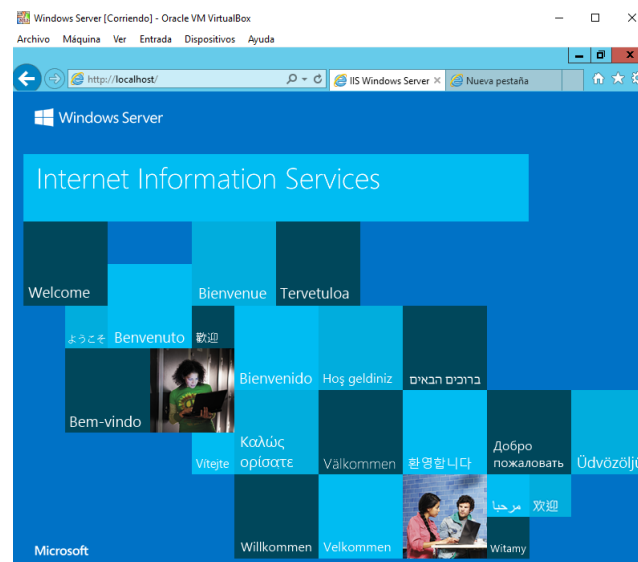


Figura 10.2: Prueba del servidor web en Windows Server

10.2. Compruebe que el servicio está funcionando accediendo a la MV a través de la anfitriona

En la parte izquierda de la Figura 10.3 se muestra la información de la lista de IPs para comprobar la dirección IP de la MV que hay que utilizar para conectarse a ella.

En la parte derecha de la misma puede verse utilizada dicha IP en el host anfitrión, comprobando que el servicio funciona correctamente

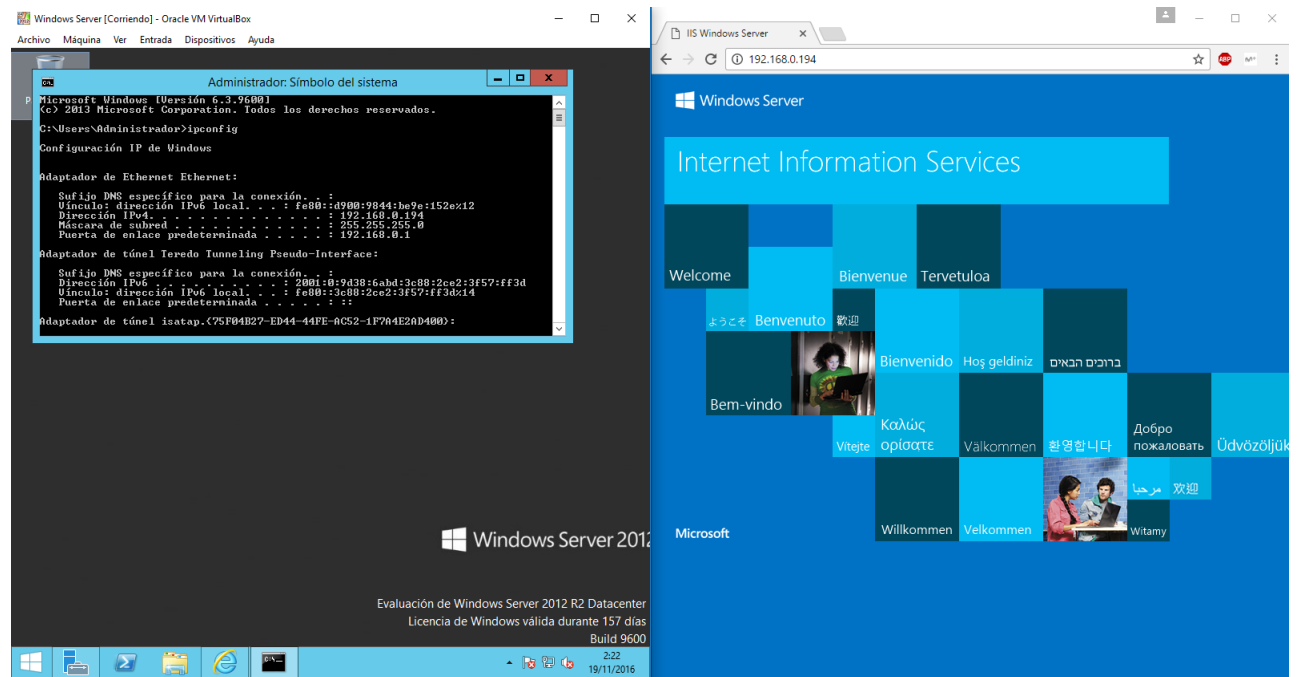


Figura 10.3: Prueba del servidor web (MV) desde la anfitriona

11. Cuestión 11

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

Hay ocasiones en las que algunas características no están incluidas en el kernel estándar debido a la falta de desarrollo o de un posible desacuerdo con los desarrolladores del mismo. Tales características pueden ser distribuidas en forma de parches.

Debian distribuye algunos de estos parches en paquetes `linux-patch-*` o `kernel-patch-*`. Estos paquetes se instalan los archivos en el `/usr/src/kernel-patches/`.

Una vez conocidos los detalles del uso de patch, se aplicará el patch **grsecurity2** a un kernel en Debian [19] mediante las siguientes órdenes:

```
> cd ~/kernel/linux-source-3.16  
> make clean  
> zcat /usr/src/kernel-patches/diffs/grsecurity2/grsecurity-3.0-3.17.1-  
201410250027.patch.gz | patch -p1
```

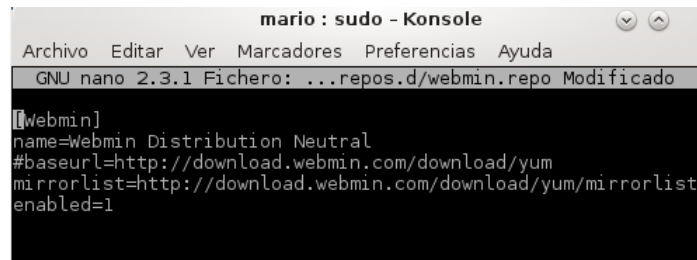
12. Cuestión 12

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.

12.1. Instalación de Webmin en CentOS

[30]

- Creación de un fichero tipo *webmin.repo* en */etc/yum.repos.d/*, Figura 12.1:

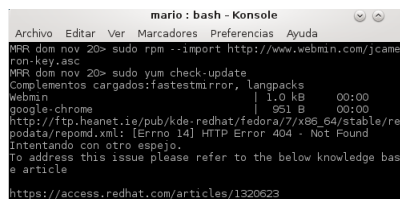


```
mario : sudo - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
GNU nano 2.3.1 Fichero: ...repos.d/webmin.repo Modificado

[webmin]
name=Webmin Distribution Neutral
#baseurl=http://download.webmin.com/download/yum
mirrorlist=http://download.webmin.com/download/yum/mirrorlist
enabled=1
```

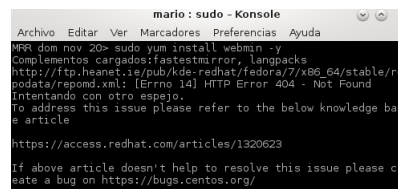
Figura 12.1: Creación de */etc/yum.repos.d/webmin.repo*

- Instalación de la clave GPC Webmin y de la herramienta, Figura 12.2:



```
mario : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR dom nov 20> sudo rpm --import http://www.webmin.com/jcameron-key.asc
MRR dom nov 20> sudo yum check-update
Complementos cargados:fastestmirror, langpacks
webmin | 1.0 kB | 991 B | 00:00
http://ftp.heanet.ie/pub/kde-redhat/fedora/7/x86_64/stable/repo
podata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Intentando con otro espejo.
To address this issue please refer to the below knowledge base article
https://access.redhat.com/articles/1320623
```

(a) Instalación de la clave GPC

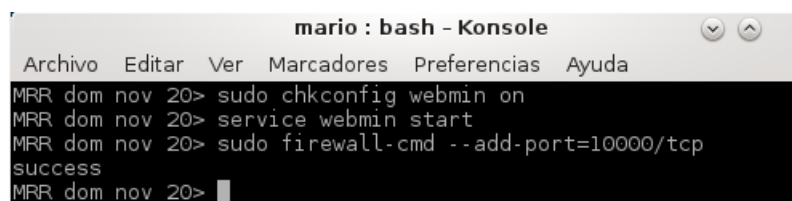


```
mario : sudo - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR dom nov 20> sudo yum install webmin -y
Complementos cargados:fastestmirror, langpacks
http://ftp.heanet.ie/pub/kde-redhat/fedora/7/x86_64/stable/repo
podata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Intentando con otro espejo.
To address this issue please refer to the below knowledge base article
https://access.redhat.com/articles/1320623
If above article doesn't help to resolve this issue please create a bug on https://bugs.centos.org/
```

(b) Instalación de la herramienta Webmin

Figura 12.2: Instalación de la clave GPC Webmin y de la herramienta.

- Inicio, automatización del servicio y apertura del puerto necesario (**10000/tcp**), Figura 12.3:



```
mario : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR dom nov 20> sudo chkconfig webmin on
MRR dom nov 20> service webmin start
MRR dom nov 20> sudo firewall-cmd --add-port=10000/tcp
success
MRR dom nov 20> █
```

Figura 12.3: Inicio, automatización del servicio y apertura del puerto necesario para Webmin

12.2. Ejecución de Webmin en CentOS

- Inicio de la herramienta desde el navegador:

Acceso mediante los datos de administrador, , Figura 12.4.

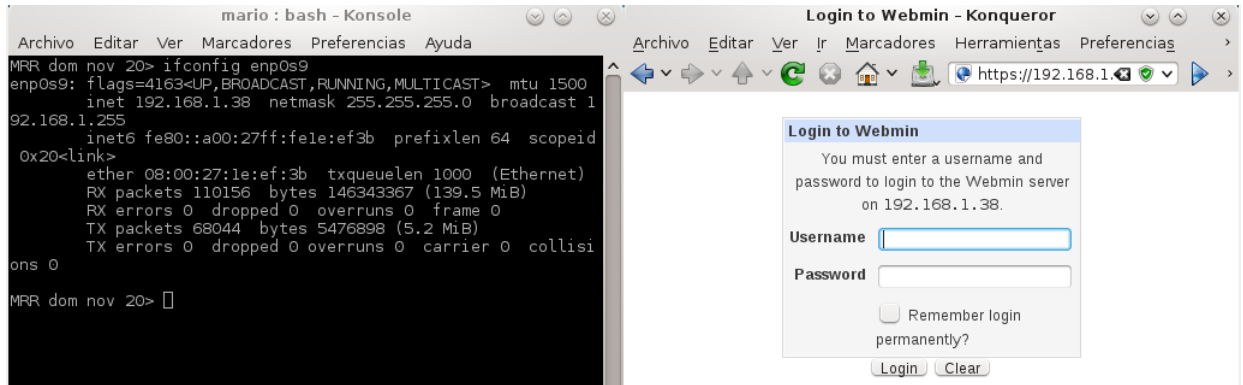


Figura 12.4: Inicio de Webmin a través del navegador.

- Información del sistema, Figura 12.5:

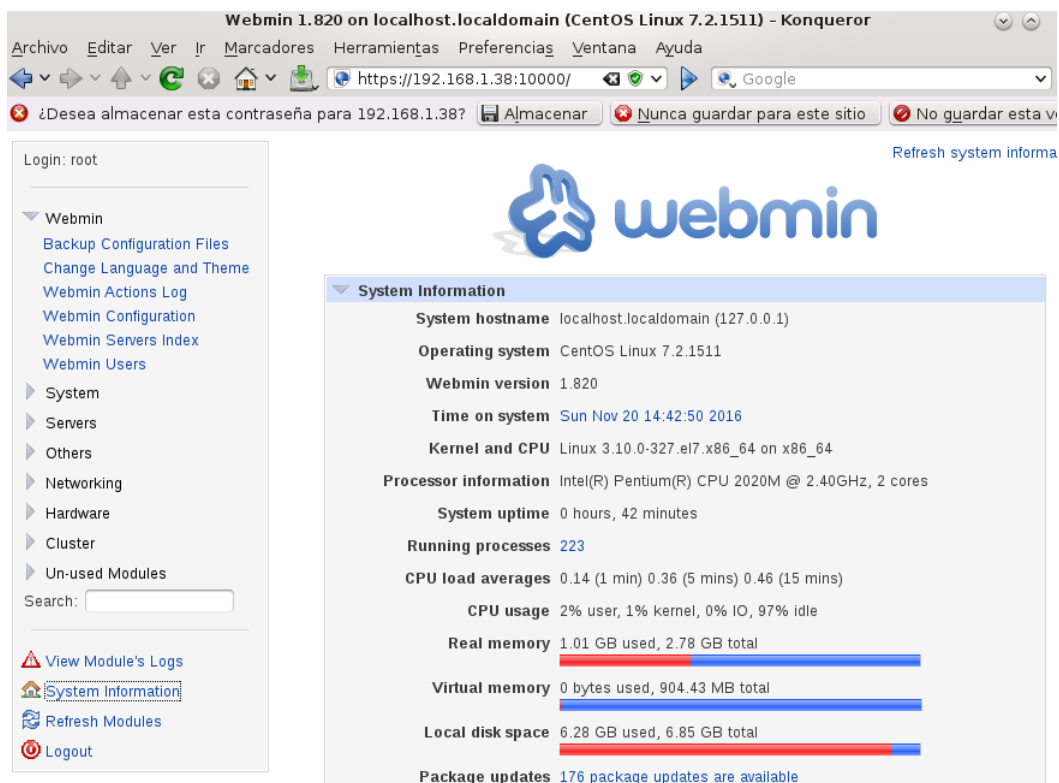


Figura 12.5: Información del sistema desde Webmin

12.3. Apertura de puertos en CentOS desde Webmin

- Apertura de puertos, Figura 12.6:

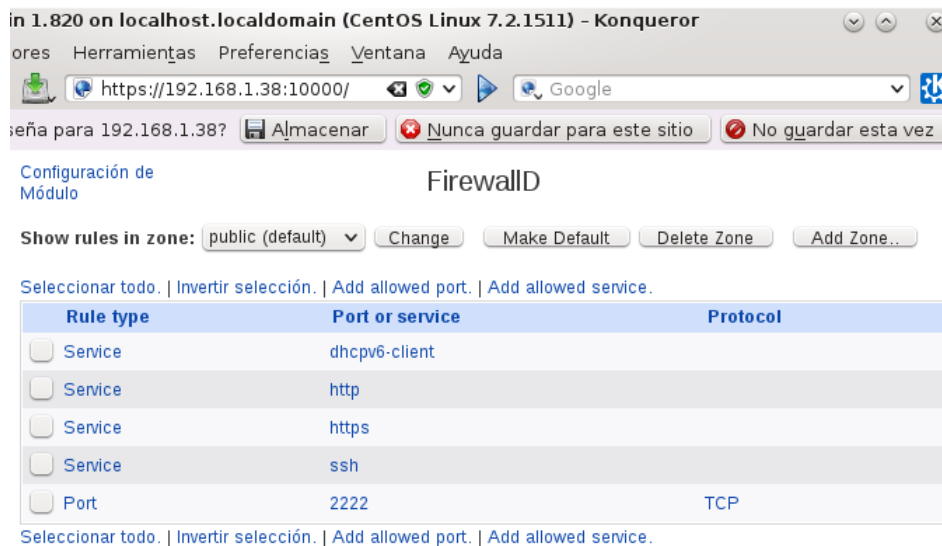
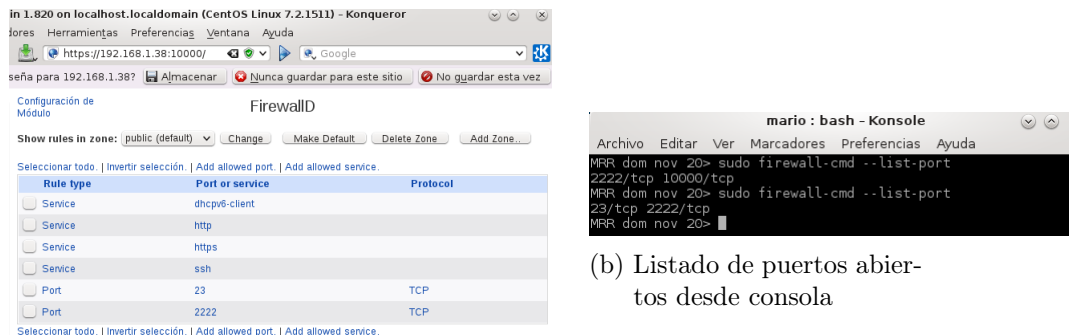


Figura 12.6: Puertos abiertos en el sistema

- Apertura del puerto necesario para **telnet**:

Prueba de la apertura de un puerto para verificar el funcionamiento de la herramienta, Figura 12.7.



- (a) Apertura del puerto 23 desde Webmin

- (b) Listado de puertos abiertos desde consola

Figura 12.7: Apertura del puerto de telnet desde Webmin

En la Figura 12.7 puede verse el listado de puertos desde consola antes y después de la modificación a través de Webmin.

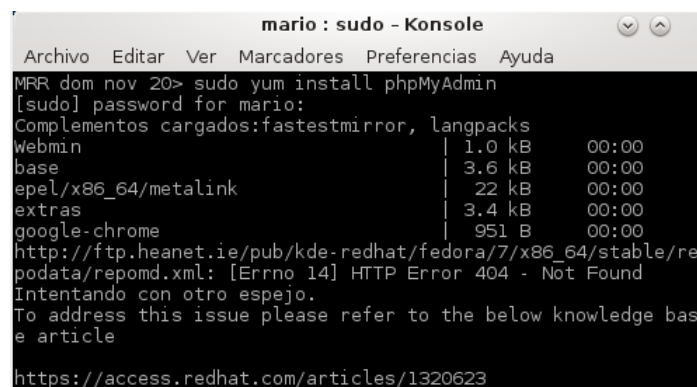
13. Cuestión 13

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.

13.1. Instalación de phpMyAdmin en CentOS

[31, 30]

1. Instalación de phpMyAdmin en CentOS:



```
mario : sudo - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR dom nov 20> sudo yum install phpMyAdmin
[sudo] password for mario:
Complementos cargados:fastestmirror, langpacks
webmin | 1.0 kB 00:00
base | 3.6 kB 00:00
epel/x86_64/metalink | 22 kB 00:00
extras | 3.4 kB 00:00
google-chrome | 951 B 00:00
http://ftp.heanet.ie/pub/kde-redhat/fedora/7/x86_64/stable/repodata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Intentando con otro espejo.
To address this issue please refer to the below knowledge base article
https://access.redhat.com/articles/1320623
```

Figura 13.1: Orden para la instalación de phpMyAdmin en CentOS

En el caso de que la instalación de la herramienta se realizara de forma remota habría que cambiar la IP que trae por defecto en el fichero de configuración `/etc/httpd/conf.d/phpMyAdmin.conf` a través de las líneas siguientes, como las que aparecen en la Figura 13.2:

Require ip *IP_address*

Allow from *IP_address*

En *IP_address* irá la IP del host desde donde accedemos remotamente. Puede consultarse, por ejemplo, desde <http://www.cualesmiip.com/>

NOTA: Esta última parte es solamente informativa, en este caso se va a realizar de forma local.


```
mario : sudo - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
GNU nano 2.3.1 Fichero: ...f.d/phpMyAdmin.conf

# phpMyAdmin - Web based MySQL browser written in php
#
# Allows only localhost by default
#
# But allowing phpMyAdmin to anyone other than localhost sho$
# dangerous unless properly secured by SSL

Alias /phpMyAdmin /usr/share/phpMyAdmin
Alias /phpmyadmin /usr/share/phpMyAdmin

<Directory /usr/share/phpMyAdmin/>
    AddDefaultCharset UTF-8

    <IfModule mod_authz_core.c>
        # Apache 2.4
        <RequireAny>
            Require ip 127.0.0.1
            Require ip ::1
        </RequireAny>
    </IfModule>
    <IfModule !mod_authz_core.c>
        # Apache 2.2
        Order Deny,Allow
        Deny from All
        Allow from 127.0.0.1
        Allow from ::1
    </IfModule>
</Directory>

<Directory /usr/share/phpMyAdmin/setup/>
    <IfModule mod_authz_core.c>
        # Apache 2.4
        <RequireAny>
            Require ip 127.0.0.1
```

Figura 13.2: Cambio de la IP para acceder de forma remota a phpMyAdmin

2. Reinicio del servicio Apache para efectuar los cambios:

> **sudo service httpd restart**

3. Inicio de phpMyAdmin desde el navegador en **http://localhost/phpmyadmin/**:
Para identificarse hay que utilizar los datos de administrador como en la Figura 13.3.

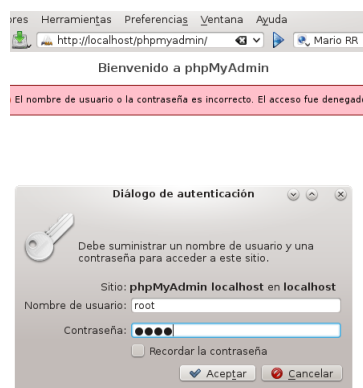


Figura 13.3: Inicio y autenticación en phpMyAdmin

4. Prueba del servicio, algo parecido al contenido de la Figura 13.4.:

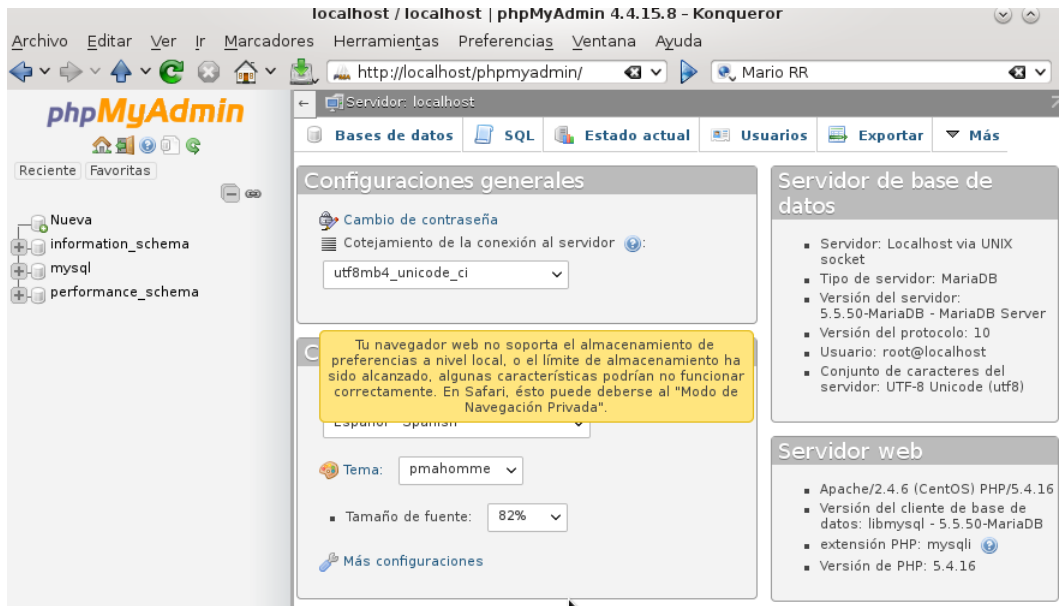


Figura 13.4: Pantalla principal de phpMyAdmin

13.2. Configuración de PHP para importar BDs de hasta 25MiB

[21]

Como se aprecia en la Figura 13.5 el tamaño máximo para importar BDs es de 2MB.

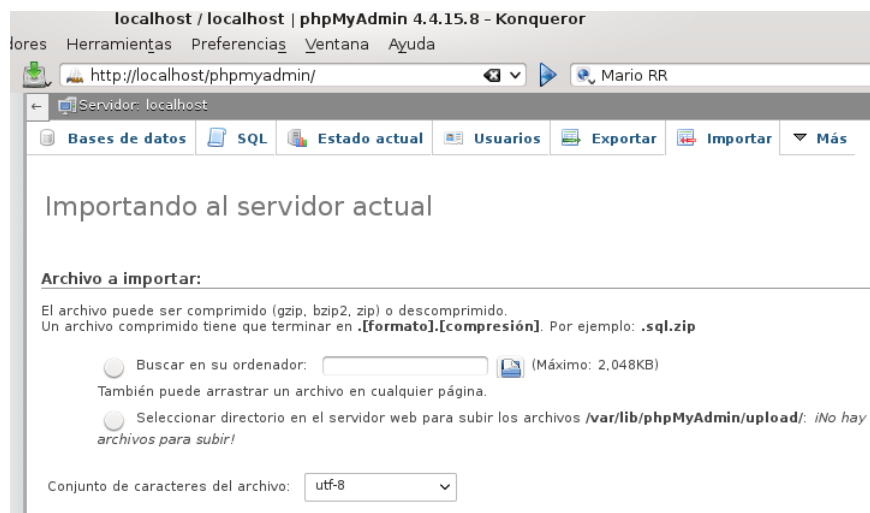
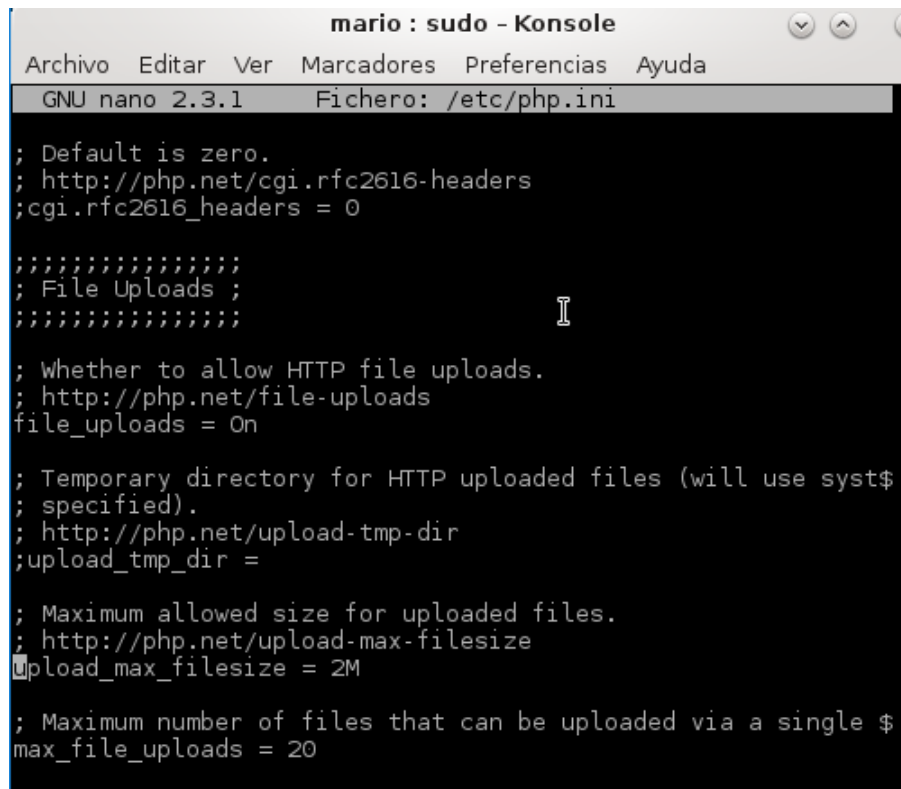


Figura 13.5: Tamaño máximo inicial de archivos a importar en phpMyAdmin

Para poder importar BDs de hasta 25MiB hay que modificar dos lineas del fichero de configuración **/etc/php.ini**:

upload_max_filesize = 25M

post_max_size = 25M



```
mario : sudo - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
GNU nano 2.3.1  Fichero: /etc/php.ini

; Default is zero.
; http://php.net/cgi.rfc2616-headers
;cgi.rfc2616_headers = 0

;;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;;

; Whether to allow HTTP file uploads.
; http://php.net/file-uploads
file_uploads = On

; Temporary directory for HTTP uploaded files (will use syst$
; specified).
; http://php.net/upload-tmp-dir
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
; http://php.net/upload-max-filesize
Upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single $
max_file_uploads = 20
```

Figura 13.6: Fichero de configuración de phpMyAdmin

Por último, para que los cambios realizados puedan verse efectuados hay que reiniciar el servicio Apache. Para ello basta con ejecutar la orden siguiente por consola:

> sudo service httpd restart

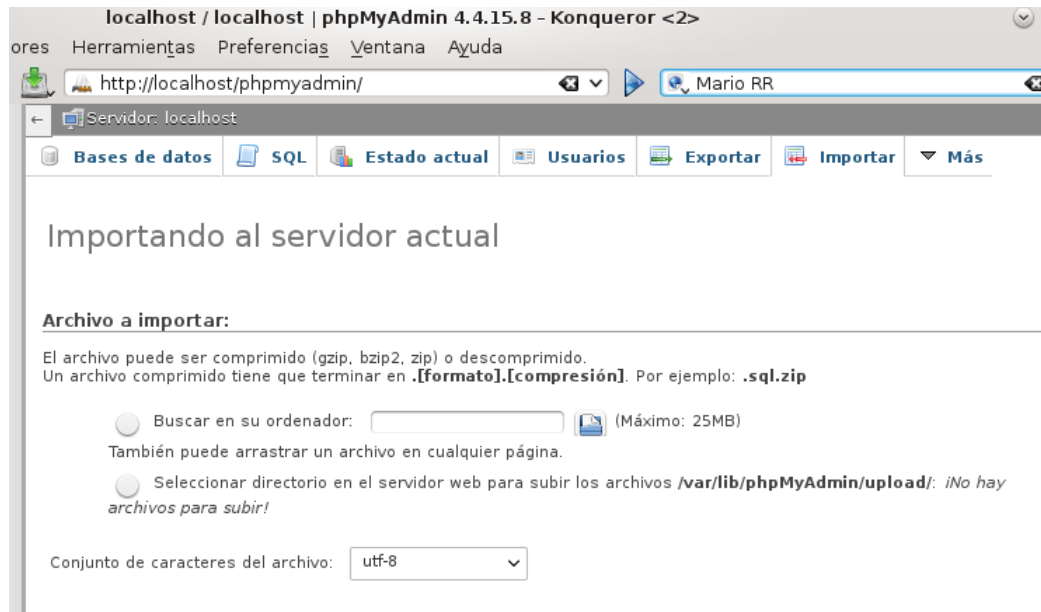


Figura 13.7: Tamaño máximo actualizado de archivos a importar en phpMyAdmin

Ya puede apreciarse cómo ha cambiado el tamaño máximo del archivo de importación en la Figura 13.7

14. Cuestión 14

Visite 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.

La web visitada ha sido <http://www.ispconfig.org/>.

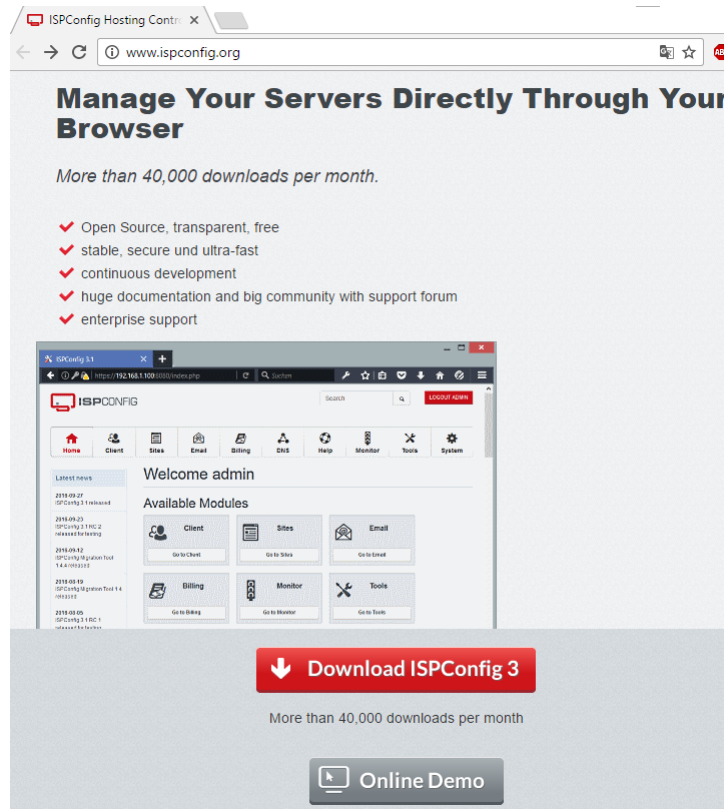


Figura 14.1: Página principal de **ispconfig**

En primer lugar, para poder acceder a una demo hay que pulsar en la parte baja de la página principal en el botón "Online Demo", como muestra la Figura 14.1.

Una vez en dicho espacio, como lo que interesa es tener recursos de administrador, se pulsará el link <http://demo3.ispconfig.org/> que dará lugar a algo parecido a la Figura 14.2 y posteriormente se introducirán los siguientes datos para la identificación:

Username: **admin**

Password: **demo**

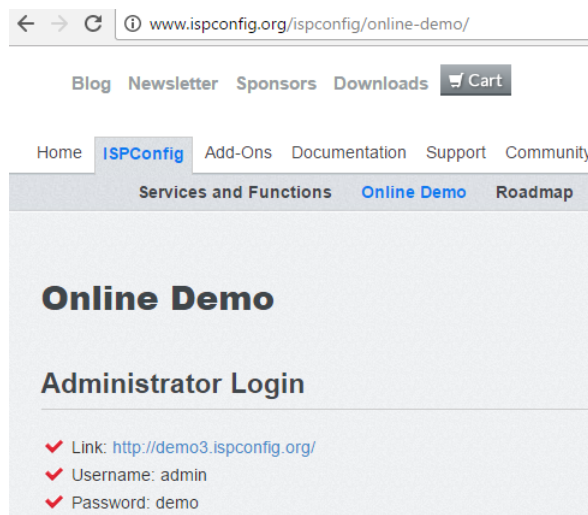


Figura 14.2: Login para administrador online demo en ispconfig

Introducidos los datos correctamente, aparecerá la página principal de la demo que ofrece el sitio. Algo como la Figura 14.3

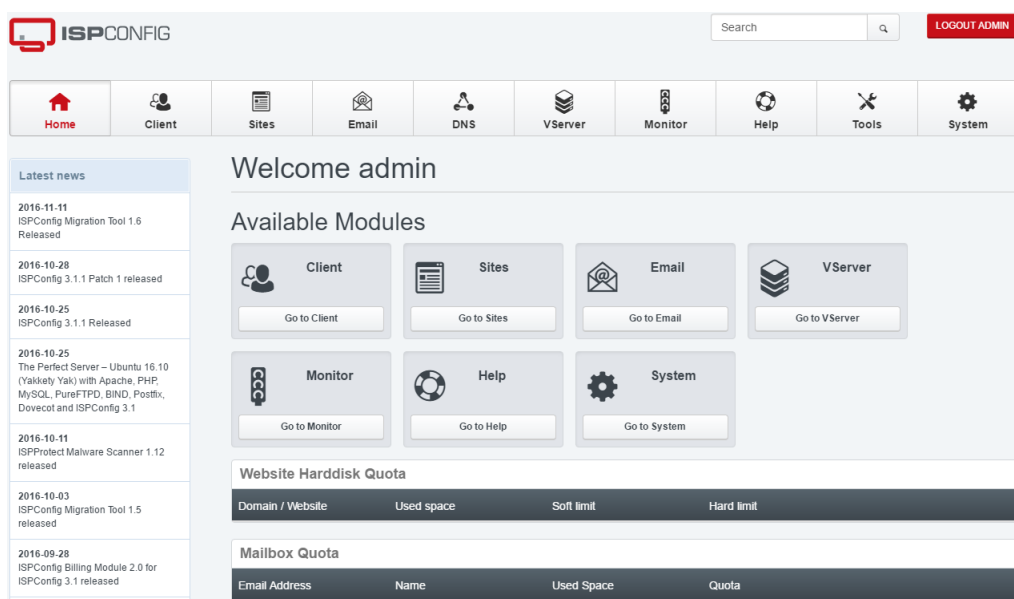


Figura 14.3: Página principal de la demo de administrador de **ispconfig**

Tanto en la parte de arriba en forma de pestañas, como en el cuerpo de la web, aparecen los módulos de configuración disponibles en este sistema. Si se elige alguno producirá a una nueva pantalla de administración.

A continuación se mostrará un ejemplo para añadir un nuevo cliente.

Pulsando sobre *Clients* y a continuación sobre *Add client* aparecerá una ficha para rellenar como la de la Figura 14.4

Figura 14.4: Añadir un cliente en la demo de ipsconfig

Una vez rellenos los datos, aceptados y aplicados por el sistema aparecerá el nuevo cliente en la lista de clientes. Véase la Figura 14.5

ID	Company name	Contact name	Customer No.	Username	City	Country
1		A		A		Portugal
3		A		A		Portugal
4	Supermercado Tal	Apellido	C4	prueba		Afghanistan

Figura 14.5: Lista de clientes actualizada en la demo de ipsconfig

Una opción interesante que ofrece este sistema es la de **monitorización**. Ésta hace que pueda sacarse un informe de errores organizados y clasificados en un tiempo de refresco específico para llevar un control en tiempo real del estado del servidor. Un ejemplo de ello es la Figura 14.6

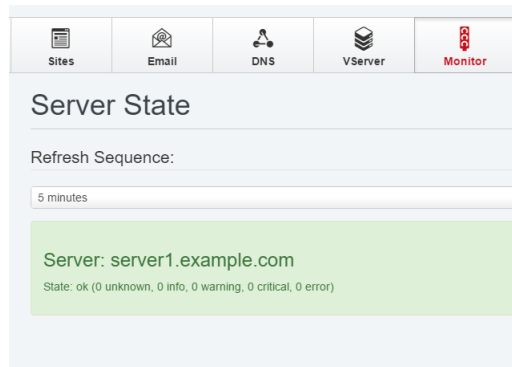


Figura 14.6: Estado del servidor en la demo online de ipconfig

Es posible cambiar el idioma de sitio desde *Tools - Password and Language*, Figura 14.7

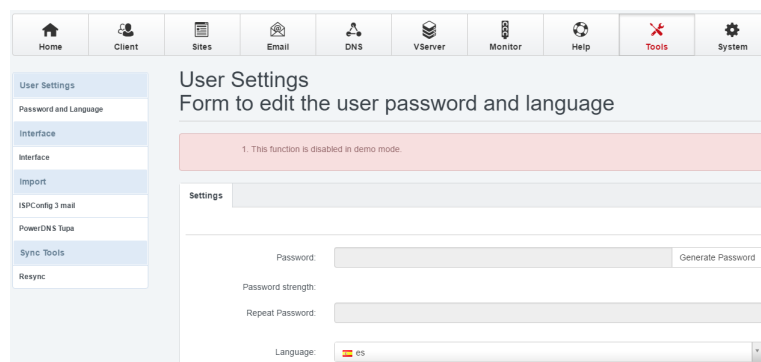


Figura 14.7: Cambio de idioma de la demo de ipconfig

Este cambio produce un error argumentando que esta función está deshabilitada para el modo demo pero, a pesar de ello, el idioma se modifica. En la Figura 14.8 puede apreciarse que ahora el idioma del sistema está en español.



Figura 14.8: Cambio de idioma realizado de la demo de ipconfig

15. Cuestión 15

15.1. Ejecute los ejemplos de find, grep

Los ejemplos aparecen en la Figura 15.1.

En primer lugar se prueba el funcionamiento de **grep** en el que se muestra la información del proceso firefox (descartando el resto de información).

En segundo lugar se prueba **find**, que copiará todos los archivos cuyo nombre termine en pdf y los copia en la carpeta /home/mario/PDFs

```
MRR jue nov 24> ps -Af | grep firefox
mario  12967  4413 35 02:21 ?        00:01:01 /usr/lib64/fi
refox/firefox
mario  13122  6776  0 02:24 pts/1    00:00:00 grep --color=
auto firefox
MRR jue nov 24> ls
Descargas  Escritorio  Música      Público     Videos
Documentos Imágenes    Plantillas  test.pdf
MRR jue nov 24> mkdir PDFs
MRR jue nov 24> find /home/mario/ -name '*pdf' -exec cp {} ~/
PDFs \;
MRR jue nov 24> ls PDFs/
test.pdf
MRR jue nov 24> █
```

Figura 15.1: Prueba de ejecución de find y grep

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

[23]

```
1 #!/bin/bash
2
3 echo "Cambiano el puerto de ssh..."
4 sed -i "/Port / c Port $1" /etc/ssh/sshd_config
5 echo "Puerto ssh modificado. Su nuevo valor es $1"
6
7 echo "Reinicio del servicio ssh para efectuar cambios..."
8 service sshd restart
```

fuentes/scriptSed.sh

El script modifica el puerto que tenga especificado el servicio ssh por uno pasado como argumento y, a continuación, reinicia el servicio.

El uso del script puede verse en la Figura 15.2, en la que en primer lugar se comprueba que el puerto actual; a continuación se ejecuta el script y por último se comprueba que el puerto se haya modificado correctamente.

```
prueba : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR lun nov 21> sudo cat /etc/ssh/sshd_config | grep Port
#Port 22
#GatewayPorts no
MRR lun nov 21> sudo ./ejercicio18.sh 1232
Cambiando el puerto de ssh...
Puerto ssh modificado. Su nuevo valor es 1232
Reinicio del servicio ssh para efectuar cambios...
Redirecting to /bin/systemctl restart sshd.service
MRR lun nov 21> sudo cat /etc/ssh/sshd_config | grep Port
Port 1232
#GatewayPorts no
MRR lun nov 21> █
```

Figura 15.2: Script que cambia el puerto de ssh

15.3. Muestre un ejemplo de uso para awk

Uso de **awk** [7] para mostrar todas las líneas del fichero `/etc/ssh/sshd_config` cuyo segundo campo contenga el número **22**.

```
> awk '$2 ~ /22/' /etc/ssh/sshd_config
```

Vista de la ejecución en la Figura 15.3

```
prueba : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR lun nov 21> sudo awk '$2 ~ /22/' /etc/ssh/sshd_config
Port 22
MRR lun nov 21> █
```

Figura 15.3: Script en Bash que cambia el puerto de ssh

16. Cuestión 16

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

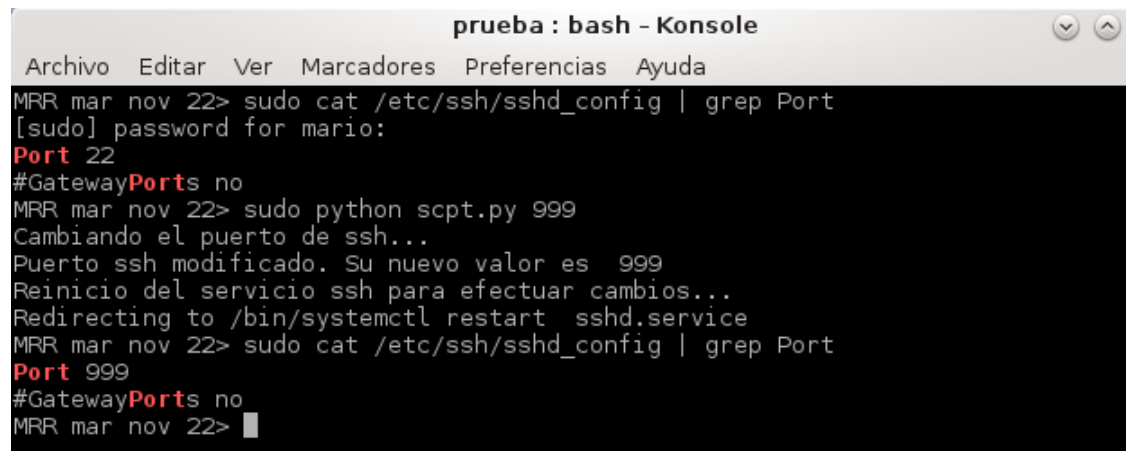
[29]

```
1  #!/usr/bin/python
2
3  import os
4  import sys
5
6  nuevo = sys.argv[1]
7
8  os.chdir("/etc/ssh/")
9  f = open("sshd_config", 'r')
10 chain = f.read()
11
12 print "Cambiando el puerto de ssh..."
13 chain = chain.replace("Port 22", "Port " + nuevo)
14 f.close()
15
16 otro = open("/etc/ssh/sshd_config", 'w')
17 otro.write(chain)
18 print "Puerto ssh modificado. Su nuevo valor es ", nuevo
19
20 print "Reinicio del servicio ssh para efectuar cambios..."
21 os.system('service sshd restart')
22 otro.close()
```

fuentes/sshPython.py

El script modifica el puerto que tenga especificado el servicio ssh por uno pasado como argumento y, a continuación, reinicia el servicio.

El uso del script puede verse en la Figura 15.2, en la que en primer lugar se comprueba que el puerto actual; a continuación se ejecuta el script y por último se comprueba que el puerto se haya modificado correctamente.



```
prueba : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR mar nov 22> sudo cat /etc/ssh/sshd_config | grep Port
[sudo] password for mario:
Port 22
#GatewayPorts no
MRR mar nov 22> sudo python scpt.py 999
Cambiando el puerto de ssh...
Puerto ssh modificado. Su nuevo valor es  999
Reinicio del servicio ssh para efectuar cambios...
Redirecting to /bin/systemctl restart  sshd.service
MRR mar nov 22> sudo cat /etc/ssh/sshd_config | grep Port
Port 999
#GatewayPorts no
MRR mar nov 22> █
```

Figura 16.1: Script en Python que cambia el puerto de ssh

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.

El programa en ejecución que se va a parar es Internet Explorer. Como puede apreciarse en la Figura 17.1 existen hasta tres procesos ejecutándose a la vez de la misma aplicación.

> Get-Process

```
MRR: 11/22/2016 00:52:58>Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	VM(M)	CPU(s)	Id	ProcessName
56	7	1812	7652	54	0,22	1360	conhost
168	11	1636	3652	46	0,56	336	csrss
143	17	1848	17424	60	3,97	400	csrss
219	14	3684	10824	52	0,14	1748	dllhost
246	32	28796	62544	182	5,80	692	dwm
1272	64	41884	95728	517	28,38	1888	explorer
0	0	0	4	0		0	Idle
1068	170	160056	220980	430	14,97	1468	iexplore
440	45	9792	29824	192	2,28	1900	iexplore
399	30	10108	26920	187	0,44	2636	iexplore
815	19	4288	10492	40	1,41	504	lsass
170	12	2212	6612	41	0,06	1412	msdtc
479	33	79660	86368	629	3,61	2904	powershell
613	64	143200	182036	821	33,48	2284	ServerManager
199	9	2040	5552	22	1,02	496	services
52	2	280	1040	4	0,16	236	smss
366	20	3052	8856	73	0,06	988	spoolsv
360	32	7004	11136	53	0,42	396	svchost
346	15	3380	9892	45	0,19	564	svchost
357	15	3284	6948	31	0,84	596	svchost
440	19	13512	17604	63	5,47	780	svchost
1115	42	15020	28892	136	7,45	808	svchost
657	23	6112	11612	83	0,53	836	svchost
657	35	8896	17932	1154	0,88	920	svchost
332	22	9644	12504	667	0,25	1096	svchost
249	14	3716	8016	46	0,05	1300	svchost
117	10	3468	7852	41	0,17	1564	svchost
167	14	4608	8872	49	0,72	2360	svchost
680	0	108	280	3	23,78	4	System
261	30	6984	12808	249	1,41	1824	taskhostex
160	10	13304	16380	87	124,67	2132	TiWorker
101	7	1432	4560	28	0,89	2920	TrustedInstaller
138	9	1764	5192	57	0,66	708	VBService
177	14	1720	17472	96	0,20	1648	VBTray
79	8	728	3612	42	0,11	408	wininit
149	8	1200	5992	53	0,19	436	winlogon
39	4	492	2600	14	0,00	1124	wlms

```
MRR: 11/22/2016 00:54:01>
```

Figura 17.1: Información de los procesos en ejecución desde PowerShell

Mediante la orden **Stop-Process -ID *proceso*** se puede parar el proceso que se desee. En este caso se pararán los procesos 1468, 1900 y 2636, que son los que mantienen a Internet Explorer.

Una vez realizadas dichas órdenes, en la Figura 17.2 puede verse cómo han desaparecido los procesos que nos interesaban.

```
MRR: 11/22/2016 00:56:19>Stop-Process -ID 1468
MRR: 11/22/2016 00:56:23>Stop-Process -ID 1900
MRR: 11/22/2016 00:56:32>Stop-Process -ID 2636
Stop-Process : No se encuentra ningún proceso con el identificador 2636.
En línea: 1 Carácter: 1
+ Stop-Process -ID 2636
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (2636:Int32) [Stop-Process], ProcessCommandException
+ FullyQualifiedErrorId : NoProcessFoundForGivenId,Microsoft.PowerShell.Commands.StopProcessCommand

MRR: 11/22/2016 00:56:40>Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	UM(M)	CPU(s)	Id	ProcessName
56	7	1812	7656	54	0,31	1360	conhost
161	10	1636	3644	46	0,56	336	csrss
131	14	1844	14716	55	4,19	400	csrss
219	14	3684	10824	52	0,14	1748	dllhost
204	23	24004	42640	131	5,81	692	dwm
1237	62	41352	95636	516	28,47	1888	explorer
0	0	0	4	0	0	0	Idle
768	19	4204	10404	40	1,41	504	lsass
172	12	2248	6628	41	0,06	1412	msdtc
515	34	72540	80276	630	3,86	2904	powershell
599	64	143228	182052	821	33,53	2284	ServerManager
191	9	1988	5532	22	1,02	496	services
52	2	280	1040	4	0,16	236	smss
366	20	3052	8856	73	0,06	988	spoolsv
359	32	7004	11124	53	0,42	396	svchost
343	15	3328	9876	45	0,19	564	svchost
336	14	3212	6920	30	0,84	596	svchost
464	22	13888	17744	66	5,47	780	svchost
1097	42	14908	28824	135	7,45	808	svchost
652	22	6164	11620	84	0,53	836	svchost
665	35	8944	17952	1154	0,88	920	svchost
332	22	9640	12504	667	0,25	1096	svchost
249	14	3716	8012	46	0,05	1300	svchost
117	11	3520	7868	41	0,17	1564	svchost
167	14	4608	8872	49	0,72	2360	svchost
642	0	108	280	3	23,92	4	System
254	30	6952	12644	249	1,41	1824	taskhostex
138	9	1616	5096	57	0,66	708	UBoxService
177	12	1688	6532	85	0,20	1648	UBoxTray
79	8	728	3612	42	0,11	408	wininit
149	8	1200	5992	53	0,19	436	winlogon
39	4	492	2600	14	0,00	1124	wlms

```
MRR: 11/22/2016 00:56:48>
```

Figura 17.2: Parada de procesos desde PowerShell

Ha salido un error en la última orden porque el proceso ya no se encontraba disponible. Esto es porque dependía de alguno de los otros procesos que se habían eliminado antes que él y ha sido borrado de forma análoga.

18. Cuestión opcional 2

Para evitar ataques de fuerza bruta podemos usar fail2ban que mete en una lista negra las IPs que intentan iniciar sesión de manera errónea.

Instale el servicio y pruebe su funcionamiento. [1]

1. Instalación del servicio:

> **sudo yum install fail2ban**

2. Por motivos de seguridad, hay que configurar un fichero local de configuración a través de una copia del original:

> **sudo cp -pf /etc/fail2ban/jail.conf /etc/fail2ban/jail.local**

3. Modificación del fichero de configuración local según intereses:

> **sudo nano /etc/fail2ban/jail.local**

En este caso, para probar se han realizado las siguientes de la Figura 18.1:

```
# "bantime" is the number of seconds that a host is banned.
bantime = 120

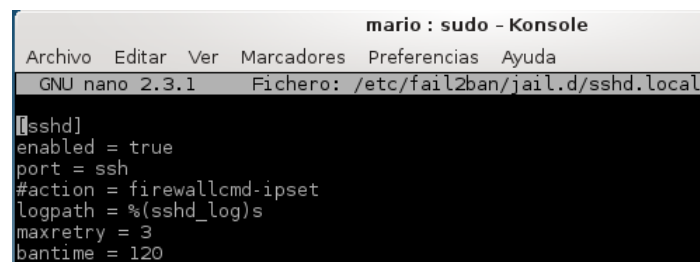
# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 600

# "maxretry" is the number of failures before a host get banned.
maxretry = 3
```

Figura 18.1: Fichero de configuración /etc/fail2ban/jail.local

4. Añadido de un archivo jail para proteger SSH, Figura 18.2:

> **sudo nano /etc/fail2ban/jail.d/sshd.local**



```
mario : sudo - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
GNU nano 2.3.1 Fichero: /etc/fail2ban/jail.d/sshd.local

[sshd]
enabled = true
port = ssh
#action = firewallcmd-ipset
logpath = %(sshd_log)s
maxretry = 3
bantime = 120
```

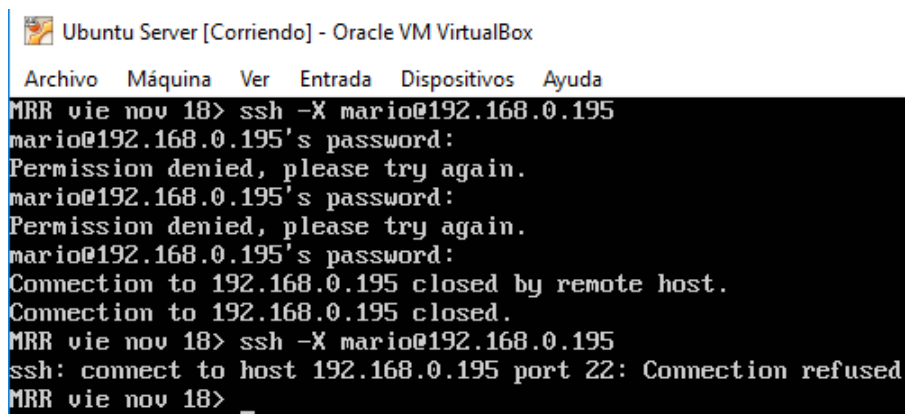
Figura 18.2: Archivo jail de protección SSH

5. Reinicio del servicio para que se efectúen los cambios.

> **sudo service fail2ban restart**

6. Prueba de funcionamiento.

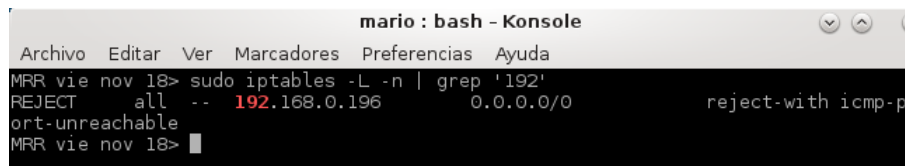
En la Figura 18.3 se muestra cómo a los dos intentos ya se no posibilita la conexión.



```
Ubuntu Server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
MRR vie nov 18> ssh -X mario@192.168.0.195
mario@192.168.0.195's password:
Permission denied, please try again.
mario@192.168.0.195's password:
Permission denied, please try again.
mario@192.168.0.195's password:
Connection to 192.168.0.195 closed by remote host.
Connection to 192.168.0.195 closed.
MRR vie nov 18> ssh -X mario@192.168.0.195
ssh: connect to host 192.168.0.195 port 22: Connection refused
MRR vie nov 18> _
```

Figura 18.3: Prueba de funcionamiento con fuerza bruta

En la Figura 18.4 se puede comprobar la IP que acaba de ser baneada.



```
mario : bash - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
MRR vie nov 18> sudo iptables -L -n | grep '192'
REJECT    all  --  192.168.0.196      0.0.0.0/0          reject-with icmp-p
ort-unreachable
MRR vie nov 18> █
```

Figura 18.4: Prueba de funcionamiento con fuerza bruta

19. Cuestión opcional 3

Instale el servicio RKhunter y pruebe su funcionamiento [5]

- Instalación del servicio RKhunter en Ubuntu Server.

Por medio del comando:

```
> sudo apt-get install rkhunter
```

```
MRR mar nov 22> sudo apt-get install rkhunter
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
binutils bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin liblockfile1
libruby2.3 libyaml-0-2 postfix rake ruby ruby-did-you-mean ruby-minitest ruby-net-telnet
ruby-power-assert ruby-test-unit ruby2.3 rubygems-integration unhide unhide.rb unzip zip
Paquetes sugeridos:
binutils-doc procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre sasl2-bin
dovecot-common postfix-cdb postfix-doc libwww-perl ri ruby-dev bundler
Se instalarán los siguientes paquetes NUEVOS:
binutils bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin liblockfile1
libruby2.3 libyaml-0-2 postfix rake rkhunter ruby ruby-did-you-mean ruby-minitest
ruby-net-telnet ruby-power-assert ruby-test-unit ruby2.3 rubygems-integration unhide unhide.rb
unzip zip
0 actualizados, 24 nuevos se instalarán, 0 para eliminar y 70 no actualizados.
4 no instalados del todo o eliminados.
Se necesita descargar 10,2 MB de archivos.
Se utilizarán 47,6 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] _
```

Figura 19.1: Instalación del servicio RKhunter en Ubuntu Server

Después de ejecutar la orden de instalación (Figura 19.1), aparecerá una ventana de configuración Postfix (Figura 19.2) en la que habrá que escoger el tipo de configuración del servidor de correo. La elección se hará en función de las necesidades.

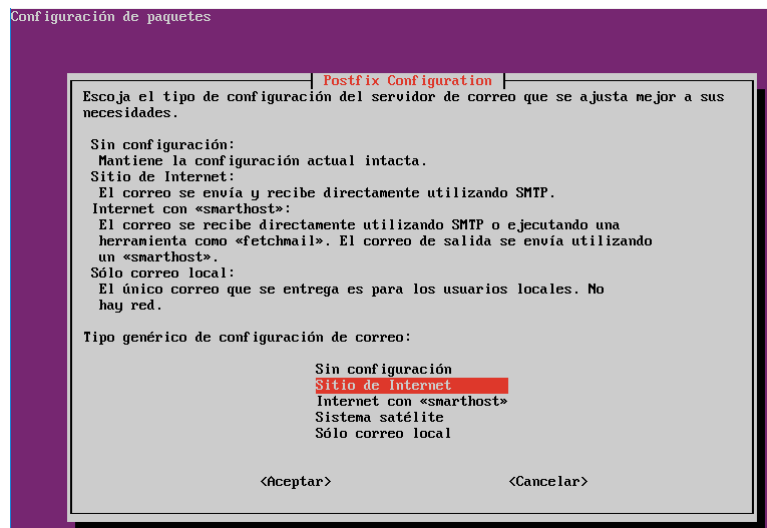


Figura 19.2: Configuración Postfix en Rhunter

Una vez finalizada la instalación, hay que actualizar los archivos de la base de datos del servicio. Estos archivos contienen información para determinar si el comportamiento de un fichero es sospechoso o no.

Para ello se ejecutará la siguiente orden (Figura 19.3):

> **sudo rkhunter --propupd**

```
MRR mar nov 22>
MRR mar nov 22> sudo rkhunter --propupd
[ Rootkit Hunter version 1.4.2 ]
File updated: searched for 177 files, found 148
MRR mar nov 22> sudo rkhunter --versioncheck
[ Rootkit Hunter version 1.4.2 ]

Checking rkhunter version...
  This version : 1.4.2
  Latest version: 1.4.2
MRR mar nov 22> _
```

Figura 19.3: Actualización de la base de datos de Rhunter

Además se comprobará que no existe una versión más reciente del servicio (Figura 19.3) mediante el comando:

> **sudo rkhunter --versioncheck**

Ahora es el momento de ejecutar el servicio por vez primera, una forma de hacerlo es a través de la orden (Figura 19.4):

> **sudo rkhunter --checkall**

```
MRR mar nov 22> sudo rkhunter --checkall
[ Rootkit Hunter version 1.4.2 ]

Checking system commands...

Performing 'strings' command checks
  Checking 'strings' command [ OK ]

Performing 'shared libraries' checks
  Checking for preloading variables [ None found ]
  Checking for preloaded libraries [ None found ]
  Checking LD_LIBRARY_PATH variable [ Not found ]

Performing file properties checks
  Checking for prerequisites [ OK ]
  /usr/sbin/adduser [ OK ]
  /usr/sbin/chroot [ OK ]
  /usr/sbin/cron [ OK ]
  /usr/sbin/groupadd [ OK ]
  /usr/sbin/groupdel [ OK ]
  /usr/sbin/groupmod [ OK ]
  /usr/sbin/grpck [ OK ]
```

Figura 19.4: Primera ejecución de Rhunter

La primera ejecución puede dar algunos mensajes de advertencia, pero no tiene por qué estar el sistema infectado. Un ejemplo de ello es lo que aparece en la Figura 19.5

```
Checking the local host...

Performing system boot checks
  Checking for local host name           [ Found ]
  Checking for system startup files       [ Found ]
  Checking system startup files for malware [ None found ]

Performing group and account checks
  Checking for passwd file                [ Found ]
  Checking for root equivalent (UID 0) accounts [ None found ]
  Checking for passwordless accounts      [ None found ]
  Checking for passwd file changes        [ Warning ]
  Checking for group file changes          [ Warning ]
  Checking root account shell history files [ None found ]

Performing system configuration file checks
  Checking for an SSH configuration file   [ Found ]
  Checking if SSH root access is allowed   [ Warning ]
  Checking if SSH protocol v1 is allowed   [ Not allowed ]
  Checking for a running system logging daemon [ Found ]
  Checking for a system logging configuration file [ Found ]
  Checking if syslog remote logging is allowed [ Not allowed ]

Performing filesystem checks
  Checking /dev for suspicious file types [ Warning ]
  Checking for hidden files and directories [ None found ]
```

Figura 19.5: Advertencias en la ejecución Rhunter

Para evitar estas advertencias, se puede reconfigurar rkhunter para que la próxima vez que se ejecute haga caso omiso de estos archivos a través de listas blancas. Esto se hace editando el archivo `/etc/rkhunter.conf` y quitando el `#` de delante de estas líneas.

```
File properties checks...
  Files checked: 148
  Suspect files: 0

Rootkit checks...
  Rootkits checked : 378
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 3 minutes and 1 second

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

MRR mar nov 22>
MRR mar nov 22>
MRR mar nov 22> cat /var/log/rkhunter.log | grep Warning
cat: /var/log/rkhunter.log: Permiso denegado
MRR mar nov 22>
MRR mar nov 22> sudo cat /var/log/rkhunter.log | grep Warning
[01:48:58] Checking for passwd file changes [ Warning ]
[01:48:58] Warning: User 'postfix' has been added to the passwd file.
[01:48:58] Checking for group file changes [ Warning ]
[01:48:58] Warning: Group 'postfix' has been added to the group file.
[01:48:58] Warning: Group 'postdrop' has been added to the group file.
[01:48:58] Checking if SSH root access is allowed [ Warning ]
[01:48:58] Warning: The SSH and rkhunter configuration options should be the same:
[01:49:00] Checking /dev for suspicious file types [ Warning ]
[01:49:00] Warning: Suspicious file types found in /dev:
MRR mar nov 22> _
```

Figura 19.6: Resultados de la ejecución de Rhunter

En la Figura 19.6 pueden verse los resultados de la ejecución de rhunter. En este caso no se ha encontrado ningún rootkit en el sistema.

Para más detalles sobre advertencias y demás puede visualizarse el log de la ejecución desde el fichero `/var/log/rkhunter.log`

20. Cuestión opcional 5

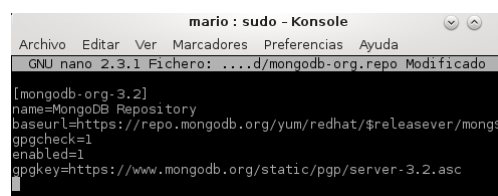
[20]

20.1. Realice la instalación de MongoDB en alguna de sus máquinas virtuales.

- Instalación de MongoDB en Centos 7:

El paquete de instalación de Mongo no existe dentro de los repositorios por defecto de Centos. A pesar de ello MongoDB dispone de un repositorio dedicado que se puede añadir al servidor.

Para ello se añade la información del repositorio con nombre `/etc/yum.repos.d/mongodb-org.repo`. A continuación se añadirán las líneas que aparecen en la Figura 20.1.



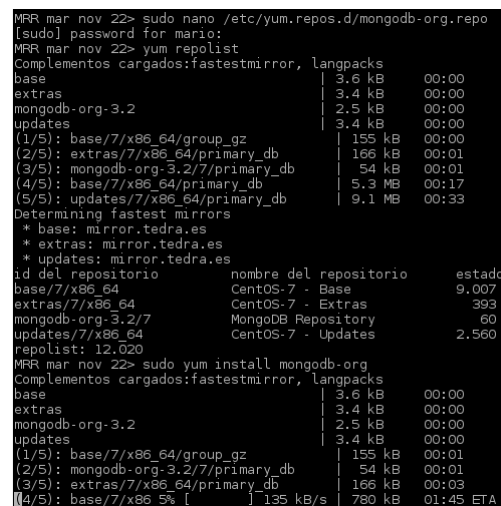
```
mario: sudo - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
GNU nano 2.3.1 Archivo: ...d/mongodb-org.repo Modificado

[mongodb-org-3.2]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongod
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-3.2.asc
```

Figura 20.1: Fichero de configuración del repositorio de MongoDB

Ahora se comprobará que el repositorio ya existe en sistema a través de la orden `yum repolist` (Figura 20.2), y seguidamente se procederá a su instalación mediante el comando:

> `sudo yum install mongodb-org`



```
MRR mar nov 22> sudo nano /etc/yum.repos.d/mongodb-org.repo
[sudo] password for mario:
MRR mar nov 22> yum repolist
Complementos cargados:fastestmirror, langpacks
base                                     | 3.6 kB    00:00
extras                                 | 3.4 kB    00:00
mongodb-org-3.2                         | 2.5 kB    00:00
updates                                 | 3.4 kB    00:00
(1/5): base/7/x86_64/group_gz          | 155 kB    00:00
(2/5): extras/7/x86_64/primary_db       | 166 kB    00:01
(3/5): mongodb-org-3.2/7/primary_db     | 54 kB     00:01
(4/5): base/7/x86_64/primary_db         | 5.3 MB    00:17
(5/5): updates/7/x86_64/primary_db      | 9.1 MB    00:33
Determining fastest mirrors
 * base: mirror.tedra.es
 * extras: mirror.tedra.es
 * updates: mirror.tedra.es
Id del repositorio      nombre del repositorio  estado
base/7/x86_64           CentOS-7 - Base         9.007
extras/7/x86_64         CentOS-7 - Extras       393
mongodb-org-3.2/7       MongoDB Repository      60
updates/7/x86_64        CentOS-7 - Updates      2.560
repolist: 12,020
MRR mar nov 22> sudo yum install mongodb-org
Complementos cargados:fastestmirror, langpacks
base                                     | 3.6 kB    00:00
extras                                 | 3.4 kB    00:00
mongodb-org-3.2                         | 2.5 kB    00:00
updates                                 | 3.4 kB    00:00
(1/5): base/7/x86_64/group_gz          | 155 kB    00:01
(2/5): mongodb-org-3.2/7/primary_db     | 54 kB     00:01
(3/5): extras/7/x86_64/primary_db       | 166 kB    00:03
(4/5): base/7/x86_64/primary_db         | 135 kB/s | 780 kB    01:45 ETA
```

Figura 20.2: Instalación de MongoDB en Centos 7

20.2. Cree una colección de documentos y haga una consulta sobre ellos.

La colección de documentos en MongoDB debe tener una estructura similar a la de aquí abajo y tendrá extensión **.json**

En esta ocasión se ha creado una colección con datos de algunas de las facultades de Granada, fichero nombrado como **colecciones.json**.

```
1  {"direccion":  
2    {"building": "2",  
3      "coord": [-76.856077, 53.848447],  
4      "calle": "Periodista Daniel Saucedo",  
5      "zipcode": "10462"},  
6    "borough": "Granada",  
7    "tipo": "Ingeniería",  
8    "name": "ETSIIT",  
9    "universidad_id": "30075441"}  
10 {"direccion":  
11   {"building": "3",  
12     "coord": [-36.856077, 20.848447],  
13     "calle": "Puentezuelas",  
14     "zipcode": "10462"},  
15   "borough": "Granada",  
16   "tipo": "Letras",  
17   "name": "Facultad de Traducción e Interpretación",  
18   "universidad_id": "30075442"}  
19 {"direccion":  
20   {"building": "4",  
21     "coord": [-47.856077, 98.848447],  
22     "calle": "Avenida de Andalucía",  
23     "zipcode": "10462"},  
24   "borough": "Granada",  
25   "tipo": "Ingeniería",  
26   "name": "Facultad de Arquitectura",  
27   "universidad_id": "30075443"}
```

Una vez creada la colección hay que importarla a Mongo. Para ello se utiliza la siguiente orden:

```
> mongoimport -db test -collection nombreColección -file ficheroColeccion.json
```

Puede ver su ejecución en la Figura 20.3

```

MRR mié nov 23>
MRR mié nov 23> mongoimport --db test --collection universidades --file coleccion.json
2016-11-23T01:17:54.947+0100    connected to: localhost
2016-11-23T01:17:54.984+0100    imported 4 documents
MRR mié nov 23> █

```

Figura 20.3: Guardado de una colección en Mongo

Una vez guardada la colección, puede ejecutarse el servicio Mongo para consultar cualquier dato sobre ésta.

En esta ocasión se ha procedido a buscar dentro de la colección **universidades**, con el límite de **un documento** y en modo **pretty** (muestra tabulados los datos). Véase la Figura 20.4

```

MRR mié nov 23> mongo
MongoDB shell version: 3.2.11
connecting to: test
Server has startup warnings:
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
0 files. Number of processes should be at least 32000 :
2016-11-22T16:59:15.610+0100 I CONTROL [initandlisten]
> db.universidades.find().limit( 1 ).pretty()
{
  "_id" : ObjectId("5834e03294d01bd38f48c091"),
  "direccion" : {
    "building" : "1",
    "coord" : [
      -73.856077,
      40.848447
    ],
    "calle" : "Severo Ochoa",
    "zipcode" : "10462"
  },
  "borough" : "Granada",
  "tipo" : "Ciencias",
  "name" : "Facultad de Ciencias",
  "universidad_id" : "30075445"
}
> █

```

Figura 20.4: Consulta de documentos de una colección en Mongo

Referencias

- [1] <https://www.servernoobs.com/centos-and-rhel-7-restart-stop-start-networking-commands/>
- [2] Docs Centos. https://www.centos.org/docs/5/html/5.1/Deployment_Guide/s1-yum-useful-commands.html.
- [3] IETF Documents. <https://tools.ietf.org/html/rfc4253>.
- [4] IETF Documents. <https://tools.ietf.org/html/rfc854>.
- [5] Ubuntu help page. <https://help.ubuntu.com/community/RKhunter>.
- [6] Ubuntu help page. <https://help.ubuntu.com/community/ApacheMySQLPHP>, consultado el 19 de noviembre de 2016.
- [7] BULMA Javier Peces. <http://www.linux-es.org/node/31>.
- [8] Linux man page. <http://man7.org/linux/man-pages/man1/yum-config-manager.1.html>.
- [9] Linux man page. <http://manpages.ubuntu.com/manpages/wily/man1/add-apt-repository.1.html>.
- [10] Linux man page. https://linux.die.net/Bash-Beginners-Guide/sect_03_01.html.
- [11] Linux man page. <https://linux.die.net/man/1/ssh-copy-id>.
- [12] Linux man page. <https://linux.die.net/man/1/ssh-keygen>.
- [13] Linux man page. <https://linux.die.net/man/5/apt.conf>.
- [14] Linux man page. https://linux.die.net/man/5/ssh_config.
- [15] Linux man page. <https://linux.die.net/man/5/yum.conf>.
- [16] Nmap man page. <https://nmap.org/book/man.html>.
- [17] OpenBsd man page. <http://man.openbsd.org/ssh>.
- [18] Ubuntu man page. <https://wiki.ubuntu.com/SystemdForUpstartUsers>.
- [19] Debian page. <https://debian-handbook.info/browse/stable/sect.kernel-compilation.html>.
- [20] Digital Ocean Community page. <https://www.digitalocean.com/community/tutorials/how-to-install-mongodb-on-centos-7>.
- [21] Drupal Community page. <https://www.drupal.org/docs/7/managing-site-performance/increase-upload-size-in-your-phpini>.

- [22] Fedora Documentation page. https://fedoraproject.org/wiki/FirewallD/es#Puertos_y_Protocolos.
- [23] ISPconfig page. <http://www.ispconfig.org/>.
- [24] RedHat Documentation page. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html.
- [25] Ubuntu Help page. https://help.ubuntu.com/community/AptGet/Howto#Setting_up_apt-get_to_use_a_http-proxy.
- [26] Ubuntu Help page. <https://help.ubuntu.com/community/Repositories/CommandLine>.
- [27] Ubuntu Help page. <https://help.ubuntu.com/community/UFW>.
- [28] Ubuntu Help page. <https://help.ubuntu.com/lts/serverguide/apt.html>.
- [29] Carlos Picca. <http://codehero.co/python-desde-cero-manejo-de-archivos/>.
- [30] Linux tutorials page. <http://lintut.com/how-to-install-webmin-on-centos-7/>.
- [31] Linux tutorials page. https://www.howtoforge.com/apache_php_mysql_on_centos_7_lamp.