

Born2beroot

Instalación de servidor sobre Debian en máquina virtual

Sumario

1. Instalación de Debian.....	4
1.1. Parámetros de configuración de VirtualBox.....	4
1.2. Descargar Debian.....	4
1.3. Instalar Debian.....	5
2. Configuración del servidor.....	19
2.1. Instalación de utilidades.....	19
a) Instalar 'sudo'.....	19
b) Activar AppArmor.....	20
c) Instalar man pages.....	20
d) Instalar SSH server.....	20
e) Instalar 'ifconfig' y otras utilidades de red.....	20
f) Instalar 'ufw' (uncomplicated firewall).....	20
g) Instalar libpam-pwquality.....	20
h) Instalar vim.....	20
2.2. Operaciones.....	20
a) Modificar PATH de 'root'.....	20
Introducción a los directorios de Linux.....	21
Estructura de directorios.....	21
b) Operaciones con AppArmor.....	23
c) Configurar 'sudo'.....	24
d) Instalar y configurar 'kdump'.....	26
e) Crear y eliminar grupos y usuarios.....	28
f) Crear grupo 'user42' y añadir usuario.....	29
g) Comprobar servicios activos.....	29
h) Permisos y propiedad de archivos.....	29
i) Buscar archivos.....	30
j) Configurar servicio SSH.....	30
k) Configurar firewall con UFW.....	31
l) Configurar política de contraseñas.....	32
m) Cambiar nombre de 'host'.....	33
n) 'Script' programable.....	34
Procesamiento de cadenas.....	34
Introducción a tareas programadas.....	36
Fuentes de datos para el script.....	37
3. Instalar servidor HTTP.....	39
3.1. Sistema de gestión de Web.....	39
3.2. Instalación y configuración de servidor HTTP.....	39
a) Instalar servidor HTTP y gestor de base de datos.....	39
b) Configuración de 'lighttpd'.....	39
3.3. Instalación y configuración de gestor de base de datos.....	40
a) Instalar gestor de base de datos mariadb-server.....	40
b) Configuración de MariaDB.....	40
c) Crear base de datos.....	40
3.4. Instalación de interprete de PHP.....	41

Guía del Proyecto Born2beroot

3.5. Instalación de CMS WordPress.....	41
4. Instalar servidor FTP.....	45
4.1. Instalación y configuración.....	45
4.2. Transferencia de archivos vía FTP.....	46
5. Fundamentos teóricos.....	47
5.1. Sistemas basados en UNIX.....	47
Evolución de los sistemas UNIX y estructura del sistema Linux.....	47
5.2. Comparativas.....	48
Comparación Centos vs Debian.....	48
Comparación SELinux vs AppArmor.....	48
Comparación 'aptitude' vs 'apt' vs 'apt-get'.....	49
5.3. Volúmenes encriptados y SSH.....	50
6. Entrega de proyecto.....	52

1. Instalación de Debian

1.1. Parámetros de configuración de VirtualBox

SISTEMA

- Chipset (PIIX3). ICH9 is for OS X Guests.
- Enable I/O APIC (Off). The use of an I/O APIC slightly increases the overhead of virtualization and therefore slows down the guest OS a little.
- Hardware Clock in UTC Time (On). UNIX-like guest OSes typically expect the hardware clock to be set to UTC.

ALMACENAMIENTO

- ISO mount in IDE Primary Master

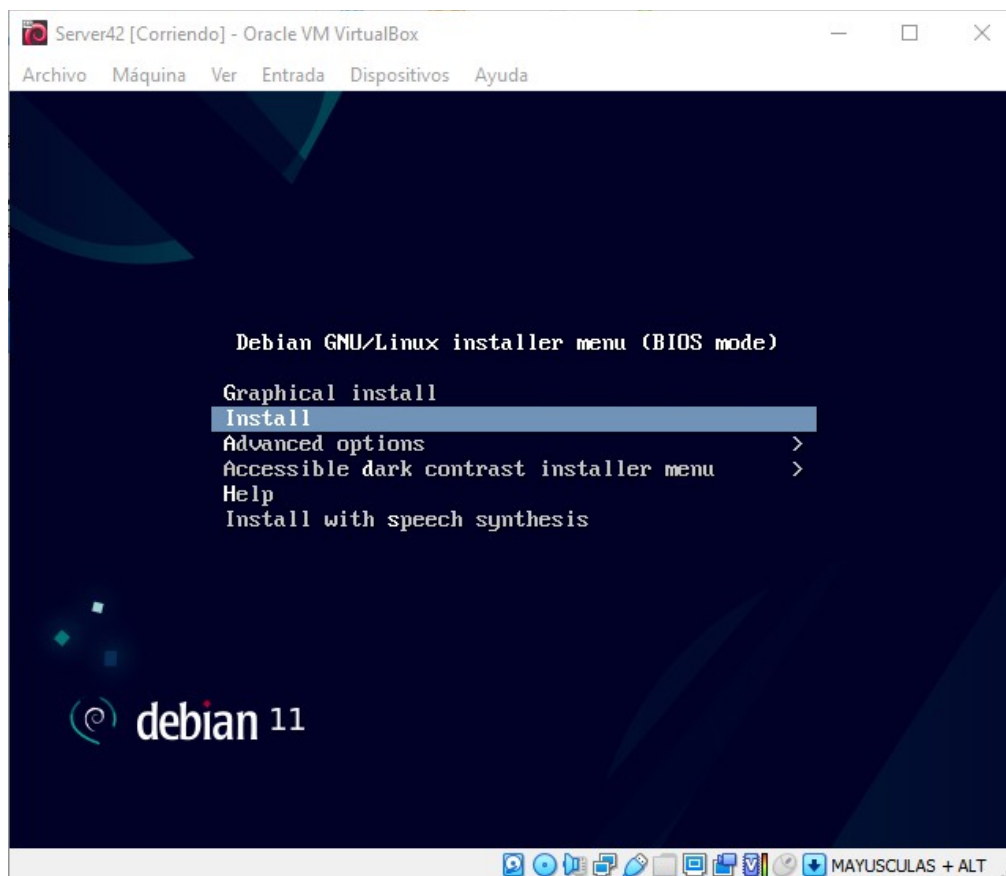
RED

- Enable Network Adapter: NAT
Avanzadas -> Reenvío de puertos -> Nueva regla -> TCP, Host Port = Guest Port = 4242 (para permitir el uso de este puerto con conexiones SSH).
- Ports -> USB (off)

1.2. Descargar Debian

Enlace: <https://www.debian.org/download> (debian-11.3.0-amd64-netinst.iso)

1.3. Instalar Debian



SELECT A LANGUAGE: *Spanish*

SELECCIONE SU UBICACIÓN: *España*

CONFIGURE EL TECLADO: *Español*

CONFIGURAR LA RED:

Nombre de la máquina: *server42*

Nombre del dominio: *server42.es*

CONFIGURAR USUARIOS Y CONTRASEÑAS:

Clave de superusuario: *******

Nombre completo para el nuevo usuario: *DavidRF*

Nombre de usuario para la cuenta: *davidrod*

Contraseña para nuevo usuario: *******

CONFIGURAR EL RELOJ: *Península*

PARTICIONADO DE DISCOS (parte obligatoria)

Guía del Proyecto Born2beroot

Guiado - utilizar todo el disco y configurar LVM cifrado

Elija disco a particionar: *SCSI2 (0, 0, 0)(sda) - 8,6 GB ATA VBOX HARDDISK*

Esquema de particionado: *Separar la partición /home*

¿Desea guardar los cambios a los discos y configurar LVM?: *Sí*

Borrando los datos en SCSI2: El instalador rellenará la partición encriptada con datos aleatorios para prevenir que se pueda filtrar meta-información del volumen cifrado.
NO CANCELAR

Frase de encriptación: *******

Cantidad en el grupo de volumen a usar en el particionado guiado: *max*

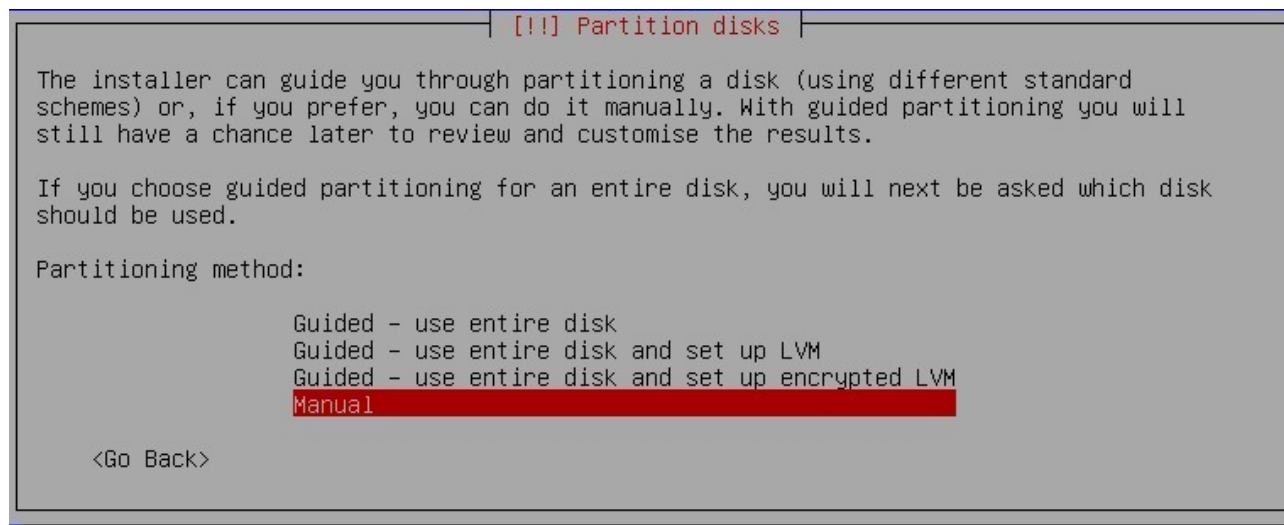
Finalizar el particionado y escribir los cambios en el disco

¿Desea escribir los cambios en los discos?: *Sí*

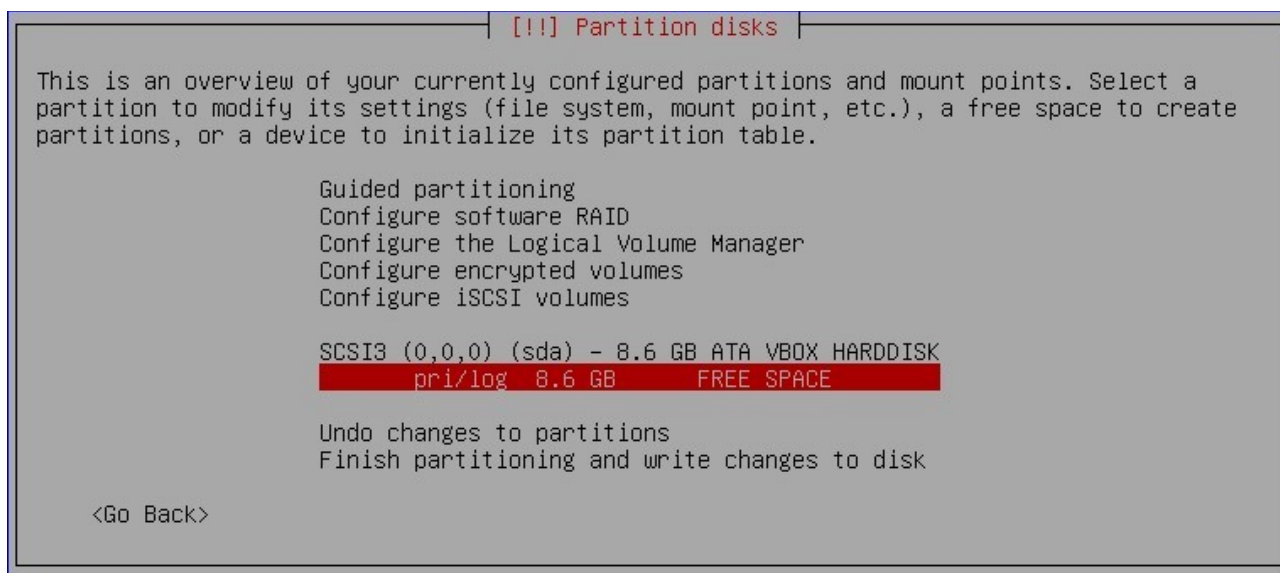
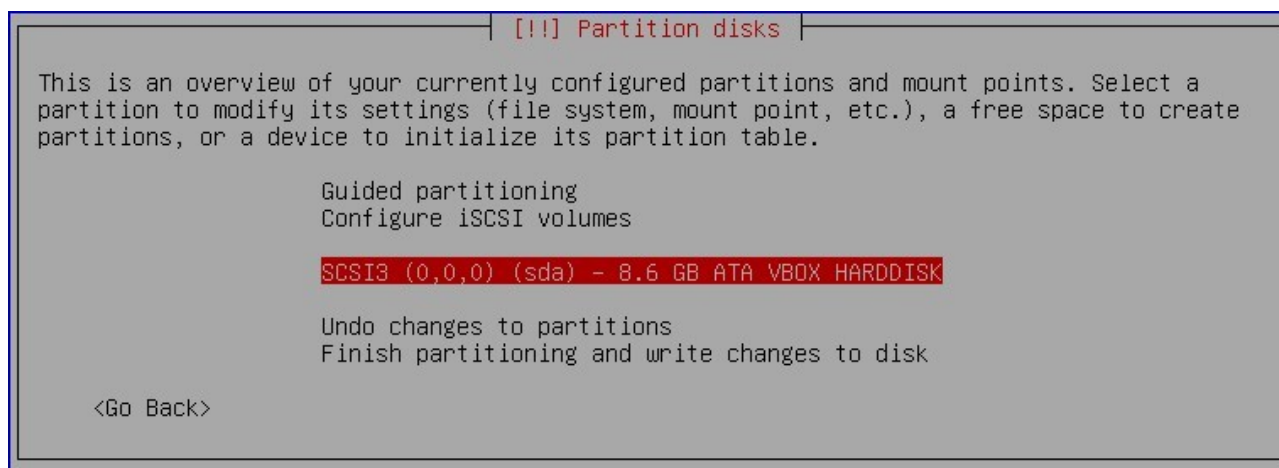
PARTICIONADO DE DISCOS (parte bonus)

Fuente: <https://www.youtube.com/watch?v=2w-2MX5QrQw>

Manual → Elegir SCSI1 (0,0,0)(sda) → Crear nueva partición vacía → Seleccionar: "pri/log 8.6GB" FREE SPACE

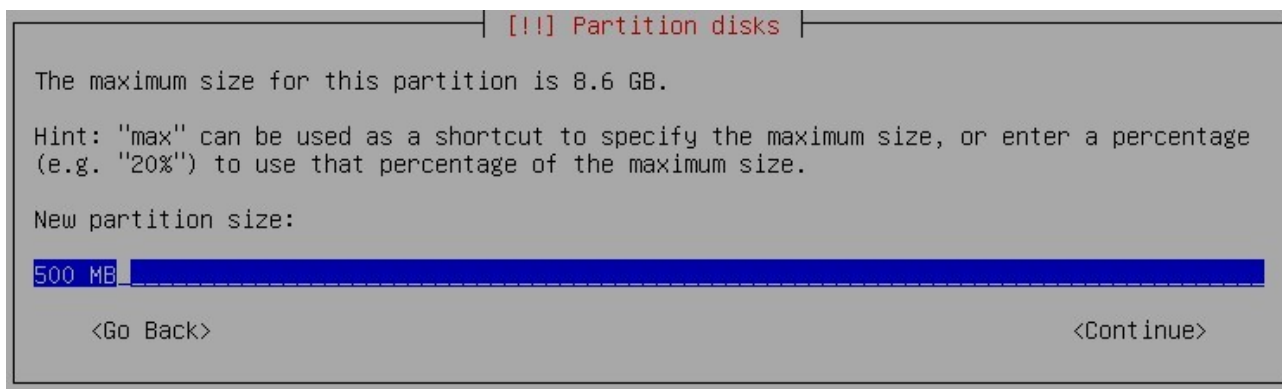


Guía del Proyecto Born2beroot

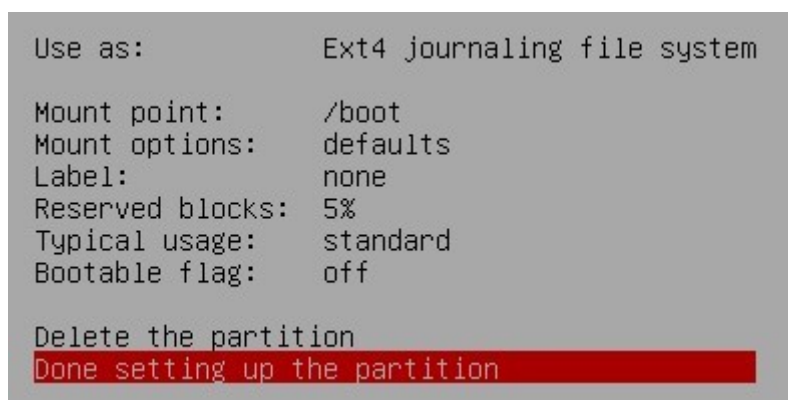
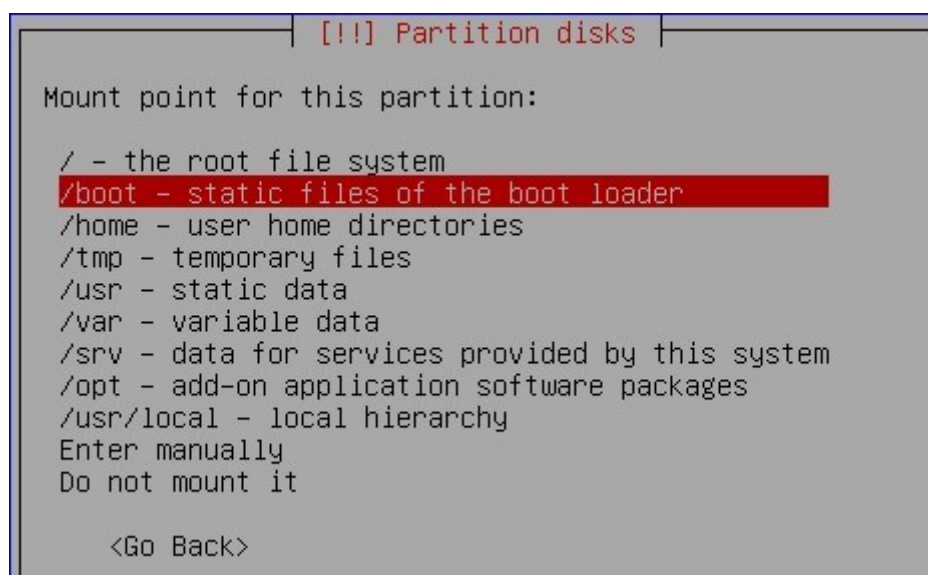
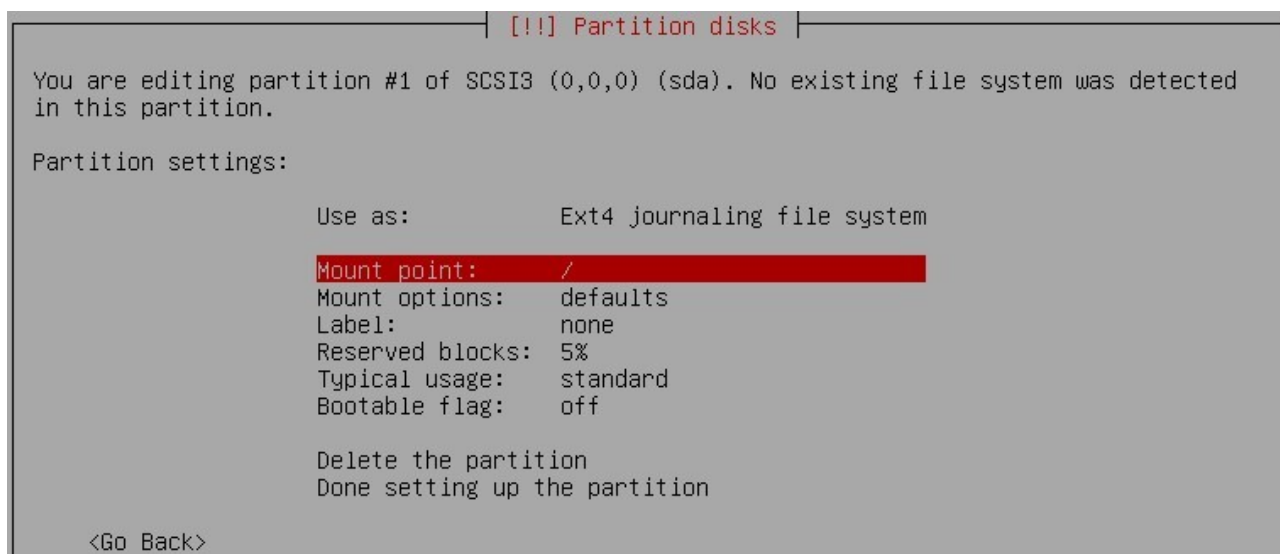


Guía del Proyecto Born2beroot

Crear nueva partición → Tamaño de nueva partición: 500M, **primaria**, localización de la nueva partición = Inicio → Configuración de la partición: Ext4, seleccionar "/" para seleccionar tipo de partición = /boot. Aceptar



Guía del Proyecto Born2beroot



Guía del Proyecto Born2beroot

NOTA: La partición /sda/sda2 la crea automáticamente con 1K de tamaño.

Vover a seleccionar FREE SPACE -> Crear nueva partición, y crear una partición **lógica** con el resto de la memoria (max) → No montar → Guardar cambios

```
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

SCSI3 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK
#1 primary 499.1 MB f ext4 /boot
pri/log 8.1 GB FREE SPACE

Undo changes to partitions
Finish partitioning and write changes to disk
```

Tamaño = max

```
[!!!] Partition disks

Type for the new partition:

Primary
Logical

<Go Back>
```

Mount point -> No montar -> Hecho

```
[!!!] Partition disks

Mount point for this partition:

/ - the root file system
/boot - static files of the boot loader
/home - user home directories
/tmp - temporary files
/usr - static data
/var - variable data
/srv - data for services provided by this system
/opt - add-on application software packages
/usr/local - local hierarchy
Enter manually
Do not mount it

<Go Back>
```

Guía del Proyecto Born2beroot

Configurar los volúmenes encriptados → Seleccionar partición deseada para encriptar → Realiza proceso de escritura aleatoria en el volumen encriptado (tarda bastante tiempo)

```
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

SCSI3 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK
#1 primary 499.1 MB f ext4 /boot
#5 logical 8.1 GB f ext4

Undo changes to partitions
Finish partitioning and write changes to disk
```

```
!!! Partition disks

Before encrypted volumes can be configured, the current partitioning scheme has to be
written to disk. These changes cannot be undone.

After the encrypted volumes have been configured, no additional changes to the partitions
on the disks containing encrypted volumes are allowed. Please decide if you are satisfied
with the current partitioning scheme for these disks before continuing.

The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #1 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as ext4

Write the changes to disk and configure encrypted volumes?

<Yes> <No>
```

```
!!! Partition disks

This menu allows you to configure encrypted volumes.

Encryption configuration actions

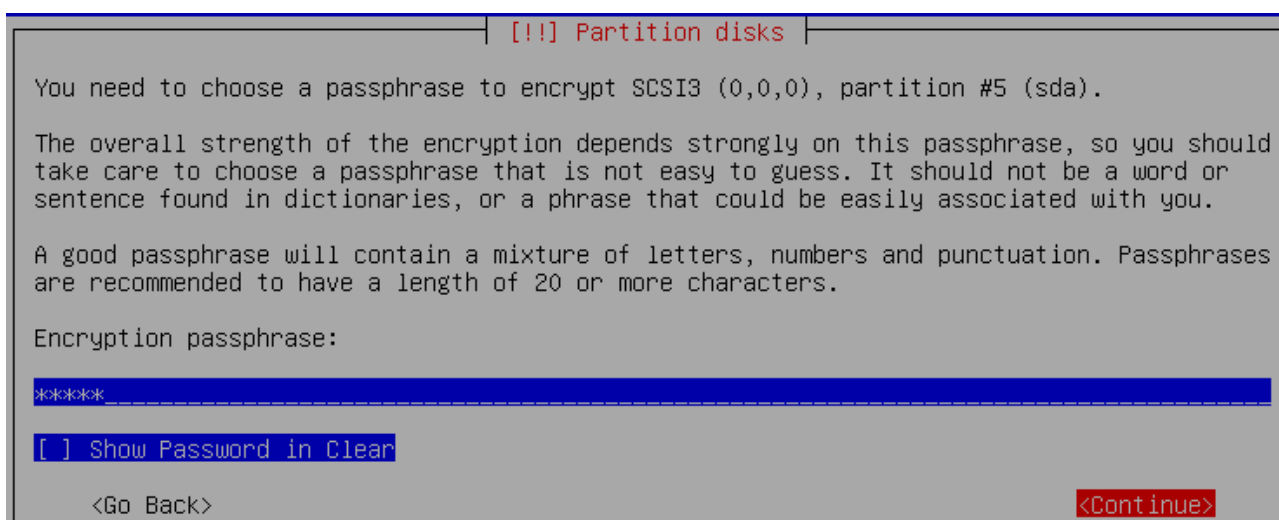
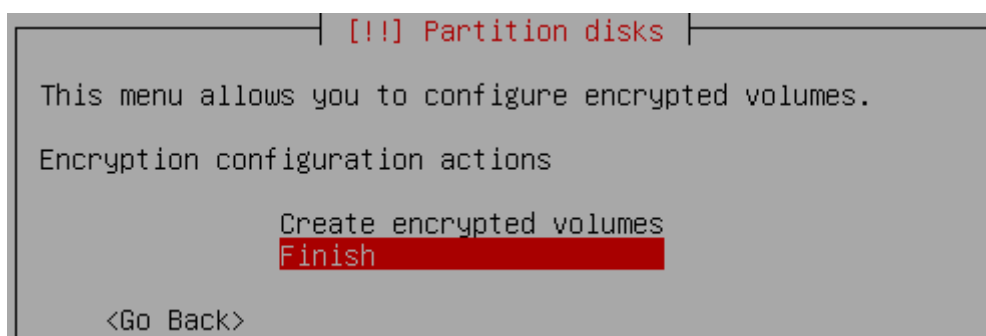
Create encrypted volumes
Finish

<Go Back>
```

Guía del Proyecto Born2beroot

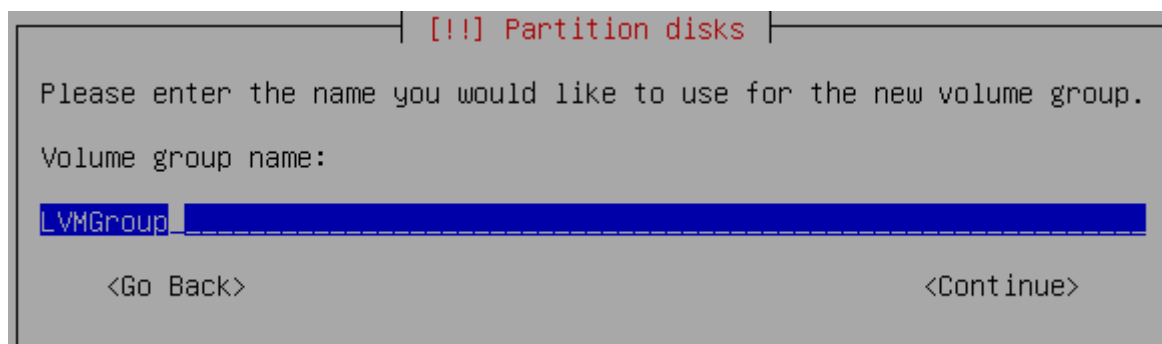
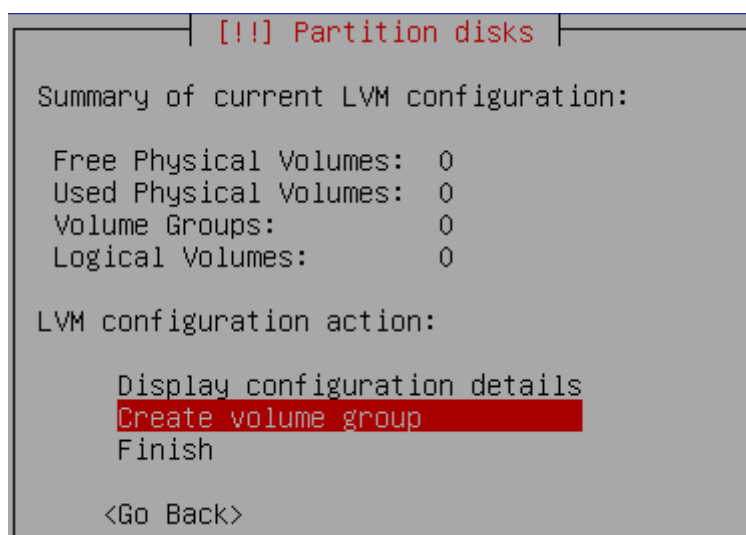
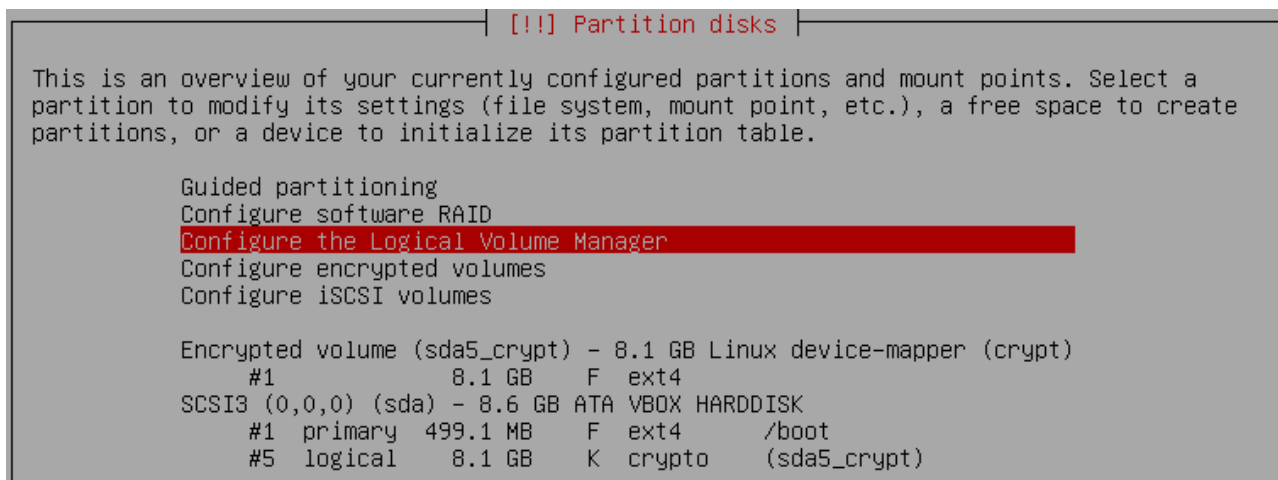


Pulsar "Done" setting up the partition".



Guía del Proyecto Born2beroot

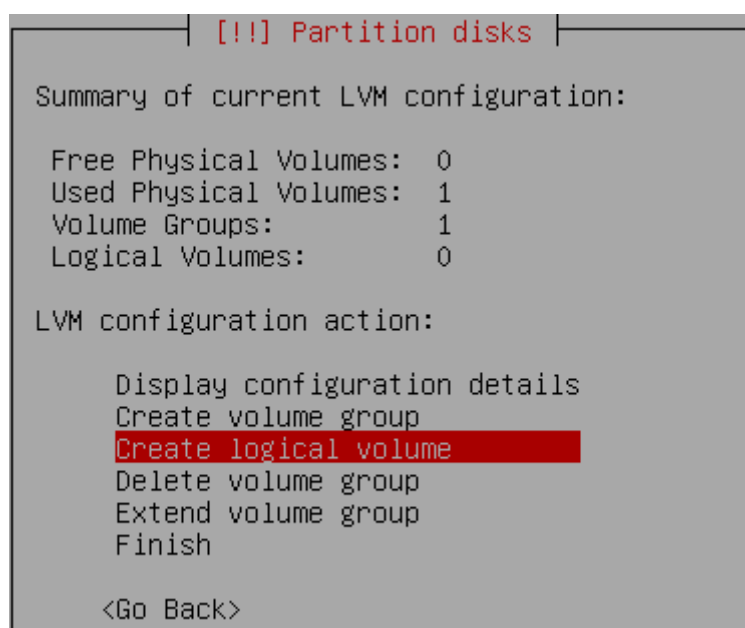
Configurar Logical Volume Manager → Crear nuevo VG (LVGroup, sin el tipo, p.e. -root)
→ Seleccionar unidad 'dev/mapper/sda5_crypt' → Crear volumen lógico (aquí se añade 'root') → Repetir con el resto de volúmenes lógicos



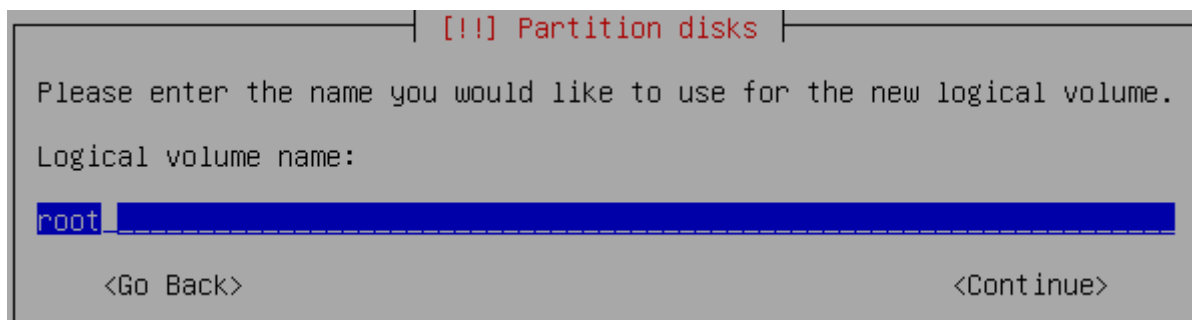
Guía del Proyecto Born2beroot



A continuación se crean los volúmenes lógicos (/root, /home, /swap...)



En siguiente ventana, elegir "LVMGroup", y después se escribe el nombre de la partición.



En la siguiente ventana fijar el tamaño.

Repetir: "Create logical volume" -> "Logical volume name" -> "Logical Volume Size", para el resto de particiones (swap, home, var, srv, tmp)

Guía del Proyecto Born2beroot

En la lista de particiones ir eligiendo cada una para formatear: “Use as: do not use” para elegir el **formato** de la partición y “Mount point” para el **punto de montaje** (/home, /var...)

Para /var/log, en “punto de montaje” elegir **montar manualmente** en /var/log.

Los discos sda1 (#1) y sda5 (#5) no se modifican.

```

[!!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

LVM VG LVMGroup, LV home - 4.1 GB Linux device-mapper (linear)
#1 4.1 GB
LVM VG LVMGroup, LV root - 998.2 MB Linux device-mapper (linear)
#1 998.2 MB
LVM VG LVMGroup, LV swap - 998.2 MB Linux device-mapper (linear)
#1 998.2 MB
LVM VG LVMGroup, LV var - 998.2 MB Linux device-mapper (linear)
#1 998.2 MB
LVM VG LVMGroup, LV var-log - 998.2 MB Linux device-mapper (linear)
#1 998.2 MB
Encrypted volume (sda5_crypt) - 8.1 GB Linux device-mapper (crypt)
SCSI3 (0,0,0) (sda) - 8.6 GB ATA VBOX HARDDISK
#1 primary 499.1 MB F ext4 /boot
#5 logical 8.1 GB K crypto (sda5_crypt)

Undo changes to partitions
Finish partitioning and write changes to disk

<Go Back>
```

```

[!!!] Partition disks

You are editing partition #1 of LVM VG LVMGroup, LV root. No existing file system was
detected in this partition.

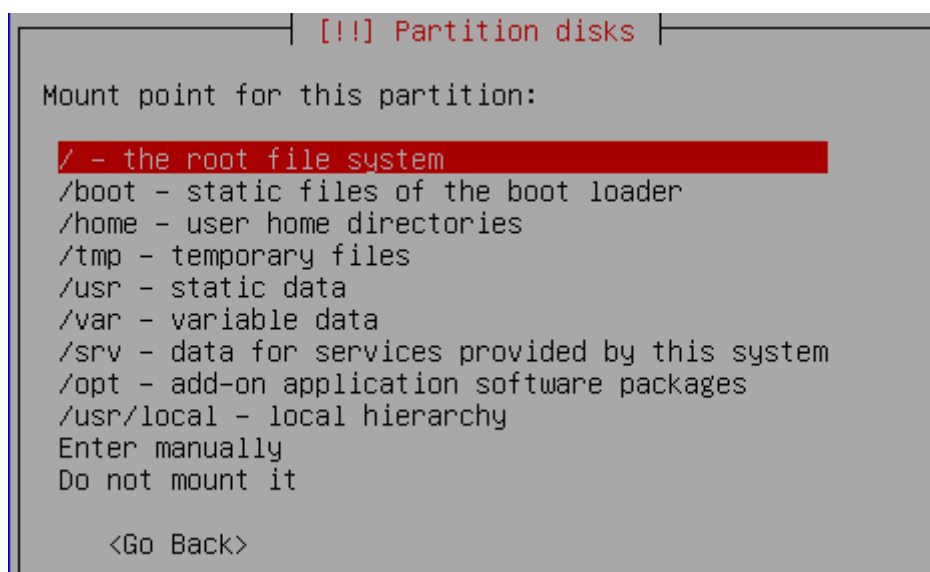
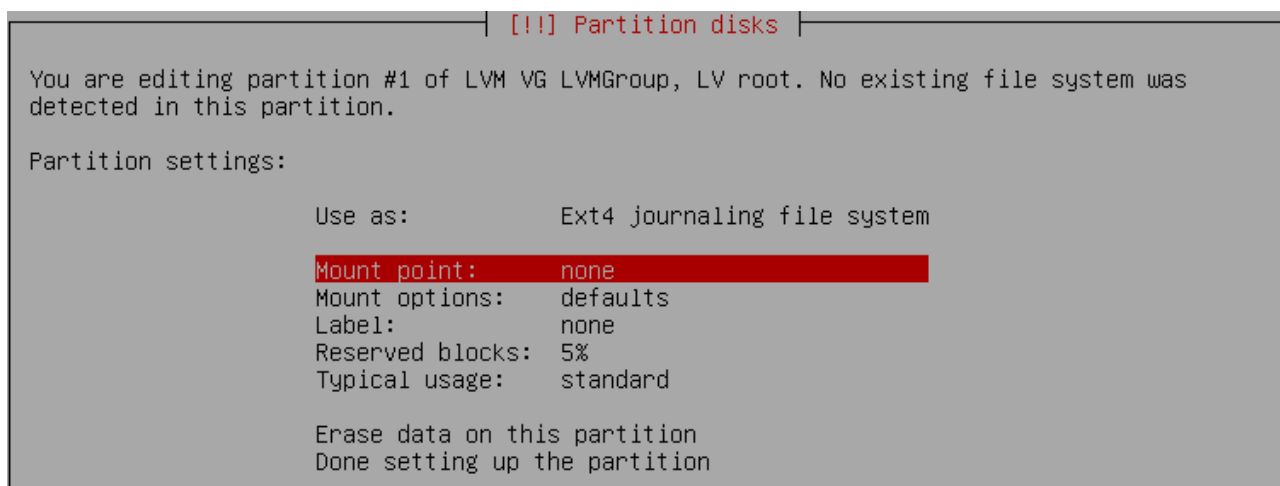
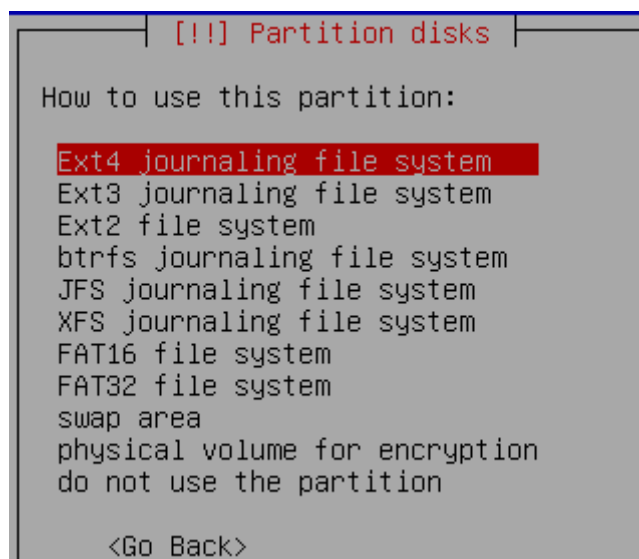
Partition settings:

Use as: do not use

Erase data on this partition
Done setting up the partition

<Go Back>
```

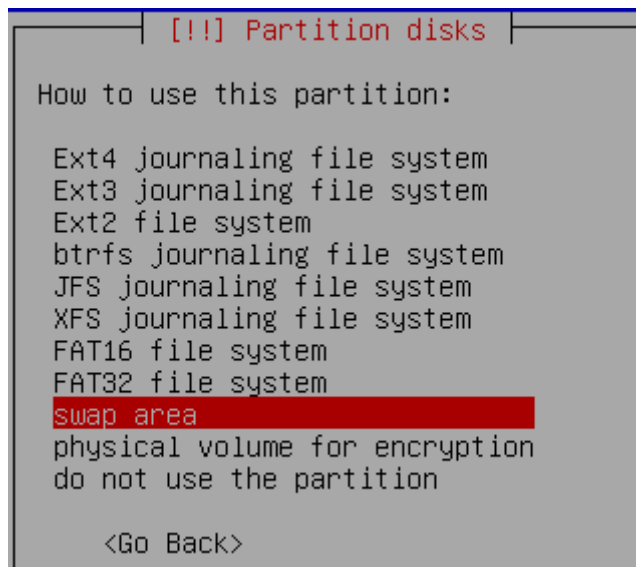
Guía del Proyecto Born2beroot



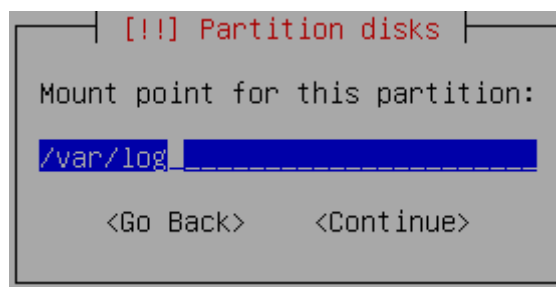
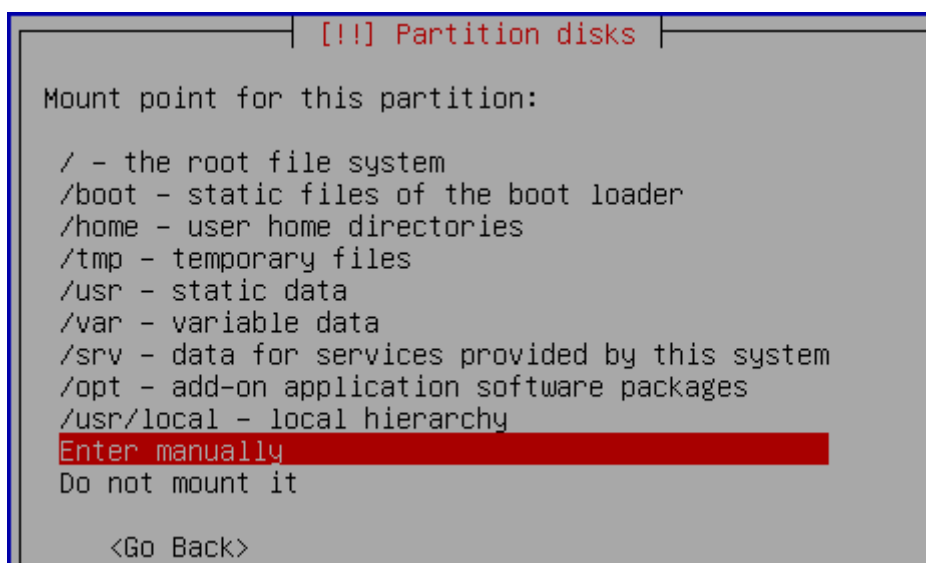
Guía del Proyecto Born2beroot

En la siguiente ventana, pulsar "Done setting up the partition" y repetir el proceso con el resto de particiones lógicas.

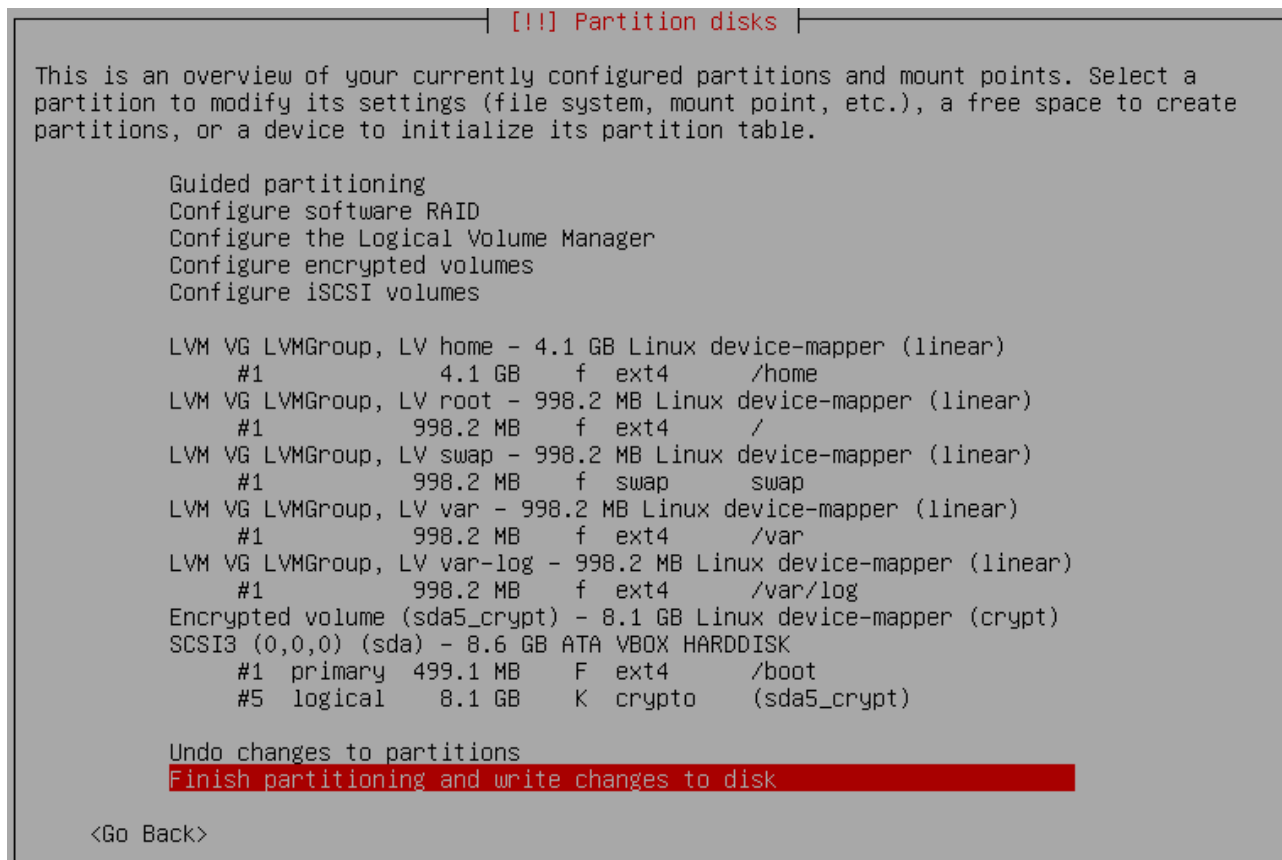
La partición 'swap' es un poco diferente ya que no se formatea ("Use as") en 'ext4':



Igualmente, para 'var-log' se formatea en 'ext4' y se realiza un montaje ("Mount point") manual:



Guía del Proyecto Born2beroot



INSTALANDO EL SISTEMA BASE

CONFIGURAR EL GESTOR DE PAQUETES

¿Desea analizar medios de instalación adicionales?: *No*

País de la réplica de Debian: *España*

Réplica de Debian: *deb.debian.org*

Información de proxy HTTP: *(dejar en blanco)*

CONFIGURACIÓN DE POPULARITY-CONTEST: *No*

SELECCIÓN DE PROGRAMAS: *(desmarcar todos los programas)*

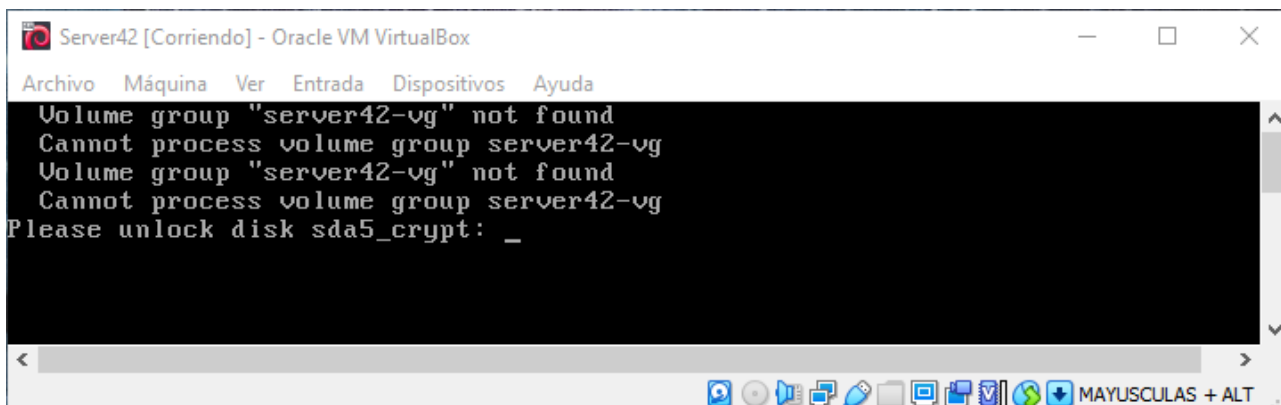
INSTALANDO EL CARGADOR DE ARRANQUE GRUB

¿Desea instalar el cargador de arranque GRUB en su unidad principal?: *Sí*

Dispositivo donde instalar el cargador de arranque: */dev/sda*

2. Configuración del servidor

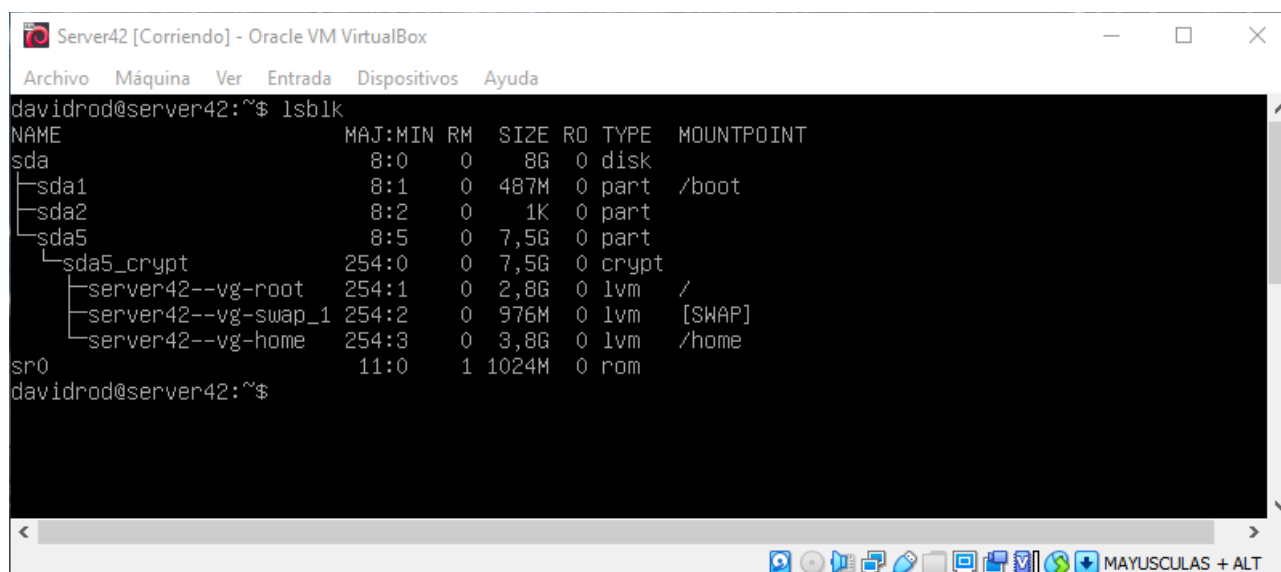
Al arrancar por primera vez la máquina virtual, pide desbloquear el disco encriptado:



```
Server42 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Volume group "server42-vg" not found
Cannot process volume group server42-vg
Volume group "server42-vg" not found
Cannot process volume group server42-vg
Please unlock disk sda5_crypt: _
```

A continuación pide credenciales de usuario (davidrod + password)

Comprobar particiones:



```
Server42 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
davidrod@server42:~$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
sda                                  8:0    0   8G  0 disk
├─sda1                              8:1    0 487M  0 part  /boot
├─sda2                              8:2    0    1K  0 part
├─sda5                              8:5    0   7.5G  0 part
│   └─sda5_crypt                    254:0    0   7.5G  0 crypt
│       ├─server42--vg-root          254:1    0   2.8G  0 lvm    /
│       ├─server42--vg-swap_1        254:2    0   976M  0 lvm    [SWAP]
│       └─server42--vg-home          254:3    0   3.8G  0 lvm    /home
└─sr0                               11:0    1 1024M  0 rom
davidrod@server42:~$
```

2.1. Instalación de utilidades

a) Instalar 'sudo'

```
su
apt update -y
apt upgrade -y
apt install sudo
```

su: Cambio a usuario 'root'
update: Resincroniza el índice de paquetes
upgrade: Actualiza los paquetes instalados en el sistema
install: Instalación del paquete que le sigue
y: Acepta todas las confirmaciones del proceso de instalación

b) Activar AppArmor

El soporte de AppArmor está ya integrado en los núcleos estándares proporcionados por Debian. Para activar AppArmor basta con instalar los siguientes paquetes:

```
sudo apt install apparmor apparmor-profiles apparmor-utils  
sudo aa-status
```

c) Instalar man pages

```
sudo apt install man-db manpages
```

d) Instalar SSH server

```
sudo apt update  
sudo apt install openssh-server
```

e) Instalar 'ifconfig' y otras utilidades de red

```
sudo apt update  
sudo apt install net-tools
```

f) Instalar 'ufw' (uncomplicated firewall)

```
sudo apt update  
sudo apt install ufw
```

g) Instalar libpam-pwquality

```
sudo apt update  
sudo apt install libpam-pwquality
```

h) Instalar vim

```
sudo apt update  
sudo apt install vim
```

2.2. Operaciones

a) Modificar PATH de 'root'

Hay que añadir direcciones al PATH para poder ejecutar algunas comandos.

Guía del Proyecto Born2beroot

```
su          # Introducir contraseña de root
export PATH=$PATH:/usr/local/sbin:/usr/sbin:/sbin
echo $PATH  #return =
usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/usr/local
/sbin:/usr:/usr/sbin:/sbin
```

También se puede escribir directamente:

```
export
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
```

Introducción a los directorios de Linux

Fuente: <https://geekland.eu/estructura-de-directorios-en-linux/>

Tipos de directorios

- a) Compartibles (C): Se pueden acceder desde **distintos equipos**
- b) No compartibles (NC): Su acceso está limitado al **administrador**
- c) Variables (V): Archivos pueden ser **modificados** sin la intervención del administrador.
- d) Estáticos (E): Archivos solo pueden ser **modificados** con la **intervención** del **administrador**.

Estructura de directorios

- a) / (raíz) :
- b) /bin (C, E): Archivos **binarios**/ejecutables necesarios para el funcionamiento del sistema. No contiene subdirectorios
- c) /boot (NC): Archivos para el **arranque** del sistema, salvo archivos de configuración. Se cargan antes de que el 'kernel' ejecute programas en modo usuario. Puede estar ubicado en su propia partición (/boot).
- d) /dev: Contiene los **dispositivos** de hardware, tratados como archivos. Ej: cdrom, sda (disco sata), audio, fd0 (disquetera)...
- e) /etc (E): Contiene los archivos (de texto) de **configuración** del sistema operativo y de programas. Estos archivos pueden ser sustituidos o complementados por archivos de configuración en /home.

Pueden existir algunas subcarpetas:

/etc/apt: Configuración de 'apt'

/etc/apt: Configuración de programas de /opt

/etc/profile: Configuración de usuarios para abrir 'bash'

- f) /home (C, V): Archivos **personales** de usuarios, salvo 'root'. Contiene también archivos de configuración de programas. Organizado por usuarios (/home/davidrod). Se suele colocar en partición propia para que una reinstalación del sistema no le afecte.
- g) /lib (C, E): Contiene **bibliotecas compartidas** necesarias para los programas de /bin y /sbin. También contiene módulos de 'kernel' y controladores de 'drivers'.
- h) /mnt: Contiene puntos de **montaje** de dispositivos de **almacenamiento** (discos duros externos, particiones de unidades externas...)
- i) /media: Contiene puntos de **montaje** de medios **extraíbles** de almacenamiento (USB, CD-ROM...)
- j) /opt (C, E): Contiene **programas ajenos** al sistema operativo (Google Chrome, Libreoffice...). Similar a /usr/local, pero aquí los programas no siguen estándares como en /usr.
- k) /proc: Sistema de archivos **virtual**. Para cada proceso activo existe un subdirectorío en la carpeta /proc, que almacena información sobre dicho proceso.
- l) /root (NC, V): Equivalente a /home para el usuario '**root**'
- m) /sbin (C, E): Archivos binarios/ejecutables que **solo** puede **ejecutar** el '**root**', para el arranque, restauración y reparación del sistema operativo.
- n) /srv: Almacena directorios y datos de **servidores**. Ej: /srv/www, /srv/ftp...
- o) /tmp: Archivos **temporales**. El sistema operativo lo vacía al reiniciar el ordenador.
- p) /usr (C, E): Contiene la mayor parte de los **programas instalados**, accesibles por todos los usuarios.

/usr/bin

/usr/include: **Cabeceras** utilizados por el software

/usr/lib: **Bibliotecas** compartidas y ficheros binarios ejecutables como 'root'

/usr/local: Contiene los archivos de /usr en un sistema de ejecución **remota**

/usr/sbin: Archivos binarios **no** esenciales para el **arranque** ni **reparar** ordenador

/usr/share: Archivos de **texto** compartibles (info, manpages, configuración, imágenes, iconos, themes...)

/usr/src: **Código fuente** de algunas aplicaciones y del 'kernel'

- q) `/var`: Contiene archivos para la **detección de problemas**. Se recomienda ubicarlo en partición propia o, al menos, fuera de la partición raíz.
 - r) `/sys`: Similar a `/proc`.
 - s) `/lost+found`: Se crea al ejecutar herramientas de **restauración** y recuperación de particiones con sistema 'ext'
-

b) Operaciones con AppArmor

Fuente: <https://debian-handbook.info/browse/es-ES/stable/sect.apparmor.html>

AppArmor aplica un conjunto de reglas (perfiles) a cada programa. El perfil aplicado por el núcleo depende de la ruta de instalación del programa a ejecutar, no del usuario. Con 'aa-status' se muestran todos los programas para los que existe perfil.

Los perfiles se pueden cargar en dos modos:

a) Enforce: Aplica las reglas y registra las tentativas de violación.

b) Complain: Solo se registran las llamadas al sistema que hubieran sido bloqueadas, pero no se bloquean realmente.

Se puede cambiar de un modo a otro, desactivar un perfil o establecerlo en modo auditoría (para que registre también las llamadas del sistema aceptadas) mediante (con permisos de root):

```
aa-enforce <program>
aa-complain <program>
aa-disable <program>
aa-audit <program>
```

La mayoría de los programas no disponen de un perfil, por lo que debe crearse uno, especialmente si se trata de programas expuestos a la red. La lista de estos programas vulnerables se obtiene mediante:

```
aa-unconfined
```

Creación de perfil

Existen una serie de utilidades para crear el perfil de una aplicación. En el siguiente ejemplo las usaremos para obtener el perfil apparmor de 'sshd' (daemon OpenSSH).

1º) Crear perfil en blanco, si no existe:

```
sudo aa-autodep sshd
```

Crea un perfil en blanco para 'sshd' en la carpeta `/etc/apparmor.d` con el nombre `usr.sbin.sshd`.

2º) Activar 'complain mode' para que 'apparmor' detecte vulnerabilidades:

```
sudo aa-complain usr.sbin.sshd
```

3º) Usar la aplicación 'sshd' mediante conexiones tipo SSH. Esto generará eventos en el archivo `/var/log/syslog`

4º) A continuación se ejecuta: `aa-logprof` que examinará el anterior archivo 'syslog' en busca de eventos relacionados con los programas cuyos perfiles se almacenan en `/etc/apparmor.d`, y preguntará al administrador acciones a realizar respecto a dichos eventos.

Se repetirán los pasos 3º) y 4º) durante un tiempo para detectar la mayor cantidad de vulnerabilidades

5º) Pasar el perfil a modo 'enforce'

```
sudo aa-enforce usr.sbin.sshd
sudo systemctl reload apparmor
```

6º) Reiniciar para que 'sshd' esté protegido (no esté en salida de `aa-unconfined`)

MUY IMPORTANTE: El ajuste de los permisos en los perfiles es complicado y si no se hace bien puede bloquear el funcionamiento de un programa. Si esto ocurre después de aplicar los pasos anteriores, ejecutar la orden:

```
sudo aa-disable <programa_con_problemas>
```

que deshabilitará el perfil de seguimiento de 'apparmor' quedando sin protección pero funcional.

c) Configurar 'sudo'

Dar permisos de 'root' a usuario al usar sudo

* Modificación de la cuenta de usuario

```
usermod -aG sudo davidrod
```

a: Añadir al usuario a un grupo suplementario

G: Grupo/s al que añadir al usuario (grupos separados por comas)

* Comprobar que el usuario se ha incluido en el grupo 'sudo'

```
getent group sudo
```

getent: Get entries from database (en este caso, de sudo)

group: 'group' database

Guía del Proyecto Born2beroot

Devuelve: `sudo:x:27:davidrod grupo sudo:x:group id (gui):usuario. 'x' indica password encriptada (no se usa realmente con grupos)`

* Dar privilegios de 'root' a usuarios

Fuente: <https://www.golinuxcloud.com/add-user-to-sudoers/>

1ª opción) Modificar directamente archivo 'sudoers'

```
su
sudo visudo
```

Edita el archivo de 'sudoers'. Añadir al archivo: `davidrod ALL=(ALL) ALL`

2ª opción) Añadir archivo en directorio /etc/sudoers.d

```
su
touch /etc/sudoers.d/custom
sudo visudo --file=/etc/sudoers.d/custom
```

touch: Modifica 'timestamp' de archivo. Si este no existe lo crea.

custom: Nombre cualquiera del archivo de extensión de 'sudoers'

Se abrirá editor al que se añadirá:

```
davidrod ALL=(ALL) ALL

usuario/grupo host=(users) list_of_commands
```

host: Host al que aplica la regla

users: Usuarios a los que aplica usuario/grupo

list_of_commands: Comandos, separados por coma, que el usuario/grupo puede ejecutar

Finalmente, es necesario **reiniciar** para que aplique la inclusión de nuevo 'sudoer'.

Configurar grupo 'sudo'

Fuente: <https://www.tecmint.com/sudoers-configurations-for-setting-sudo-in-linux/>

* Limitar el 'path' de los usuarios de 'sudo'

```
sudo visudo
```

Modificar la siguiente línea:

```
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
```

Guía del Proyecto Born2beroot

* Resto de configuración:

```
cd /etc/sudoers.d
sudo visudo --file=/etc/sudoers.d/custom
```

Limitar intentos erróneos de passwd:

```
Defaults passwd_tries=3
```

Mensaje de error:

```
Defaults badpass_message="Passwd is wrong, please try again"
```

Crear 'log file':

```
Defaults logfile="/var/log/sudo/sudo.log"
Defaults log_input, log_output # log input and output
```

Si /sudo/ no existe, créalo. Al hacerlo, con permiso sudo, emitirá un primer mensaje sobre la inexistencia de dicho archivo.

Requerir el uso de un terminal con 'login' (tty) para usar sudo:

```
Defaults requiretty
```

Este es un medio de evitar que una vulnerabilidad del servidor permita a un código malicioso hacer uso de 'sudo'. El inconveniente es que no es posible usarlo tampoco en una sesión remota con SSH.

d) Instalar y configurar 'kdump'

Fuentes:

<https://www.bentasker.co.uk/posts/documentation/linux/312-installing-and-configuring-kdump-on-debian-jessie.html>

<https://access.redhat.com/solutions/59432>

<https://www.cyberciti.biz/faq/how-to-on-enable-kernel-crash-dump-on-debian-linux/>

'kdump' es una característica del núcleo de Linux que crea **volcados** (dump) de memoria en caso de fallo catastrófico del 'kernel', con el fin de poder analizarlos para detectar sus causas.

- Instalación

```
apt install kdump-tools crash kexec-tools makedumpfile linux-  
image-$(uname -r)-dbg
```

kdump-tools	Proporciona 'init script' y 'configuration script' para automatizar 'kdump'
-------------	---

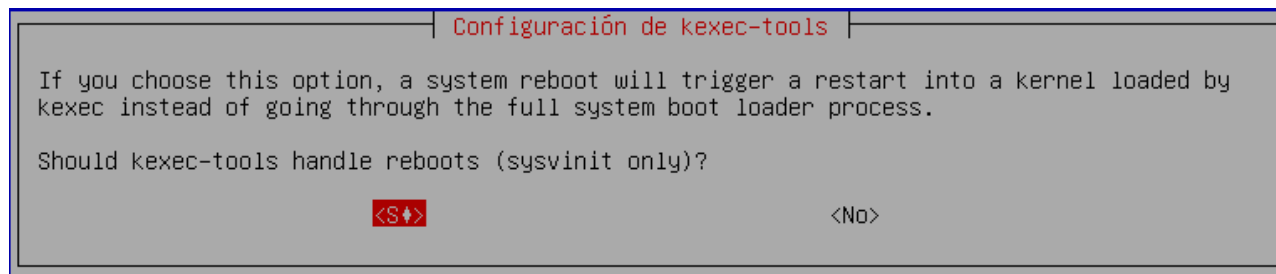
crash	Permite analizar el 'dump file' en /var/crash
-------	---

kexec-tools	Permite iniciar en un nuevo kernel desde el actual, cuando se produce un fallo catastrófico
-------------	---

Guía del Proyecto Born2beroot

`makedumpfile linux...` Crea el archivo `linux-image-5.10.0-14-amd64-dbg`
`uname -r` Imprime información del kernel (-r = versión del núcleo)

Se abrirá un configurador de paquetes para 'kexec-tools'



La siguiente ventana contiene el siguiente texto:

If you choose this option, the kdump-tools mechanism will be enabled. A reboot is still required in order to enable the crashkernel kernel parameter. Should kdump-tools be enabled by default?
Elegir: Yes

- Configuración

Archivo `/etc/default/kdump-tools`

Set `USE_KDUMP=1`

Archivo `/etc/default/grub`

`GRUB_CMDLINE_LINUX_DEFAULT="quiet crashkernel=<size>"`

ram size	crashkernel size
>0GB	128MB
>2GB	256MB
>6GB	512MB
>8GB	768MB

Actualizar 'grup': `update-grub`

Reiniciar sistema: `reboot`

e) Crear y eliminar grupos y usuarios

Fuente: <https://www.pluralsight.com/blog/tutorials/linux-add-user-command>
<https://linuxize.com/post/how-to-add-user-to-group-in-linux/>
[How to create users in Linux](#)

- Crear grupo: `groupadd <group_name>`
- Eliminar grupo: `groupdel <group_name>`
- Crear usuario y asignarlo a grupos existentes:

Opción 1ª)

```
useradd -m -g <primary_group> -G <second_grps> <new_user>
```

-m: Crea /home directory, si no existe

```
passwd <new_user> # Asignación de password
```

Opción 2ª)

```
adduser <user name> # Crea usuario y /home/<user name>
```

Solicitará: contraseña, nombre completo y otra información personal y de trabajo.

NOTA: El directorio en /home inicialmente tiene permisos go=rx.

- Asignar usuario existente a grupo primario:
`usermod -g <primary_group> <user_name>`
- Eliminar a usuario de grupo:
`gpasswd -d <user_name> <group_name>`
- Eliminar cuenta de usuario:
`userdel -r <user_name>`

Opción '-r' elimina 'home' y 'mail spool'.

- Lista de usuarios:
`cat /etc/passwd`
`more /etc/passwd`
`less /etc/passwd`

```
oracle:x:1021:1020:Oracle user:/data/network/oracle:/bin/bash
```

The diagram shows the passwd entry for 'oracle' with arrows pointing to each field and its index:

Field	Index
oracle	1
x	2
1021	3
1020	4
Oracle user	5
/data/network/oracle	6
/bin/bash	7

Teniendo la salida el siguiente formato:

- 1: Nombre de usuarios
- 2: Contraseña. 'x' indica que la contraseña se almacena en /etc/shadow
- 3: UID (ID de usuario)
- 4: GID (ID de grupo principal/primario)

- 5: Información adicional del usuarios
- 6: Directorio del usuario cuando inicie sesión
- 7: Shell predeterminado del usuario

- Lista de usuarios de un grupo:
`getent group <group_name>`
- Lista de grupos:
`groups` # Grupos del usuario activo
`groups <user>` # Grupos de usuario <user>
`getent group` # Entradas de base de datos 'group'

f) Crear grupo 'user42' y añadir usuario

```
groupadd user42
getent group user42
usermod -aG user42 <usuario existente>
```

Para crear un nuevo usuario:

```
adduser <user name> # Grupo inicial = <user name>
useradd -g<grupo inicial> <nuevo usuario>
```

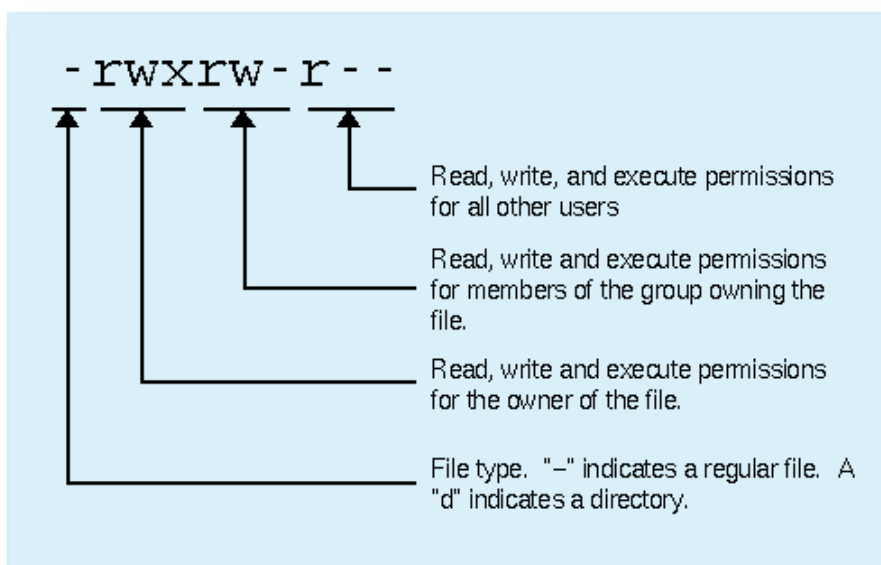
El grupo inicial (identificado por su nombre o id) debe existir.

g) Comprobar servicios activos

```
systemctl list-units --type service
systemctl status <service name>
```

h) Permisos y propiedad de archivos

- Asignar propiedad de archivo a usuario: `chown <user> <file>`
- Cambio de propietario y grupo de los archivos de subdirectorios:
`chown -R <user>:<group> path`
- Cambio de grupo propietario (misma opción recursiva de '-R')
`chgrp <group_name> <file_name>`
- Cambiar permisos de un archivo:
`chmod 755 <file_name>`
`chmod ugoa=rwx <file_name>`
Ej: `chmod u=rw, og=r <file_name>`
`u(user/owner), g(group), o(others), a(all)`
`chmod ugoa+-rwx <file_name>`
Ej: `chmod g+w <file_name>` # Añadir permiso 'w' a group



i) Buscar archivos

- Buscar archivos por nombre:
`find <path> -name <nombre admite wildcards>`
`find . -name <nombre> # Búsqueda recursiva desde dir. actual`
- Buscar archivos por contenido:
`grep <contenido> <path>`

j) Configurar servicio SSH

Fuente: <https://www.digitalocean.com/community/tutorials/how-to-use-ssh-to-connect-to-a-remote-server-es>

Lado del servidor

- Comprobar estado de SSH server:
`systemctl status ssh`
- Iniciar servicio
`systemctl start ssh`
- Reiniciar servicio
`service ssh restart`
- Cambiar configuración de SSH editando archivo `sshd_config`
`cp /etc/ssh/sshd_config{,.bak}`
`vim /etc/ssh/sshd_config`

Configuración de práctica Born2beroot:

Port 4242

Guía del Proyecto Born2beroot

```
LoginGraceTime 2m    # Tiempo máximo para acceso
PermitRootLogin no    # Impedir conectarse como root
```

Recargar configuración

```
systemctl reload ssh
```

Configurar Virtualbox

Configuración -> Red -> (Desplegar Avanzadas) Botón 'Port Forwarding'

Añadir regla:

Protocol: TCP

Host Port: 4242

Guest Port: 4242

Reiniciar máquina virtual

Lado del cliente

- Conectarse a servido mediante SSH:

```
ssh -p <port_number> <remote_username>@<server_name>
```

<server_name> será la dirección IP (en VB NAT: 127.0.0.1; si 'Adaptador puente' tendrá una dirección local 192.168.x.x)
- (Desde server) Conocer dirección IP:

```
sudo ifconfig
```

k) Configurar firewall con UFW

Fuente: <https://www.digitalocean.com/community/tutorials/como-configurar-un-firewall-con-ufw-en-ubuntu-18-04-es>

UFW es una aplicación que establece las reglas de 'iptables' que son las que determinan el comportamiento del 'firewall' de Linux

- Configurar políticas predeterminadas

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```
- Habilitar conexiones SSH

```
sudo ufw allow ssh
```

 o

```
sudo ufw allow <ssh port>
```
- Habilitar/Desabilitar/Reiniciar UFW

```
sudo ufw enable/disable/reset
```
- Eliminar reglas

```
sudo ufw status numbered
```

 # Mostrar reglas numeradas

```
sudo ufw delete <rule_number>
```

- Comprobar estado y reglas de UFW

```
sudo ufw status verbose
systemctl status ufw
```

Si está funcionando correctamente, informará (en verde): active (exited), que significa que se ha ejecutado al inicio, realizando un 'iptables-restore', y devuelve 'code=exited' al terminar.

I) Configurar política de contraseñas

Fuente: https://www.server-world.info/en/note?os=Debian_10&p=password

NOTA: Instalar y usar 'vim'.

- Configuración de archivo /etc/login.defs

```
# line 160: set 60 for Password Expiration
PASS_MAX_DAYS 30

# line 161: set 2 for Minimum number of days available
PASS_MIN_DAYS 2

# line 162: set 7 for number of days for warnings
PASS_WARN_AGE 7
```

- Configuración de archivo /etc/security/pwquality.conf

NOTA: Previamente se habrá instalado libpam-pwquality

```
# line 6
difok = 7

# line 11: uncomment and set minimum password length
minlen = 10

# line 38: uncomment and set maximum number of allowed
consecutive same characters
maxrepeat = 3

# line 20: uncomment and set minimum uppercase character
uccredit = -1

# line 15: uncomment and set minimum digit character
dcredit = -1

# line 74
enforce_for_root

# add to the end
badwords = ${USER}
```


Guía del Proyecto Born2beroot

Tras configurar la política de contraseñas, se aplicará a los nuevos usuarios que se creen. Sin embargo, no afecta a 'root' y al usuario inicial que se creó con la instalación del servidor. Esto se puede comprobar con la orden:

```
chage -l <initial_user_name>
```

```
davidrod@server:/etc$ chage -l davidrod
Último cambio de contraseña           :may 19, 2022
La contraseña caduca                   : nunca
Contraseña inactiva                    : nunca
La cuenta caduca                       : nunca
Número de días mínimo entre cambio de contraseña : 0
Número de días máximo entre cambio de contraseña : 99999
Número de días de aviso antes de que caduque la contraseña : 7
davidrod@server:/etc$
```

Como se observa, la contraseña de 'davidrod' (mi usuario inicial) tiene una caducidad de 99999 días, y número mínimo de 0 días. Además, la contraseña no caduca nunca.

Para solucionarlo se aplica el siguiente comando:

```
sudo chage -m 2 -M 30 <initial_user_name>
```

chage: Cambia expiración de contraseña de usuario

```
davidrod@server:/etc$ sudo chage -m 2 -M 30 davidrod
davidrod@server:/etc$ chage -l davidrod
Último cambio de contraseña           :may 19, 2022
La contraseña caduca                   : jun 18, 2022
Contraseña inactiva                    : nunca
La cuenta caduca                       : nunca
Número de días mínimo entre cambio de contraseña : 2
Número de días máximo entre cambio de contraseña : 30
Número de días de aviso antes de que caduque la contraseña : 7
davidrod@server:/etc$
```

Ahora la contraseña tiene fecha de caducidad.

Aplicar también a 'root', con permiso de 'sudo'.

m) Cambiar nombre de 'host'

```
hostnamectl set-hostname <new_hostname>
```

Cambiar el nuevo nombre en los archivos:

```
sudo vim /etc/hostname
sudo vim /etc/hosts
```

Comprobar nuevo nombre y reiniciar para hacerlo permanente:

```
hostnamectl  
reboot
```

n) 'Script' programable

- Escribir script de tarea y guardar en:

```
/usr/local/bin/
```

Dar permiso de ejecución para usuario

```
sudo chmod 755 <script_name>
```

- Dar permiso de ejecución al 'script' sin password, editando /etc/sudoers.d/custom:

```
<user> ALL=(root) NOPASSWD: /usr/local/bin/script.sh  
sudo reboot
```

Procesamiento de cadenas

- `grep [OPTIONS] PATTERNS [FILE]`

Busca un patrón en un archivo (o en la salida recibida de una cadena (chain)), devolviendo la línea de coincidencia.

```
Ej: hostnamectl | grep "Operating System"
```

- `uniq` # Muestra u omite líneas duplicadas

- `cut OPTION [FILE]`

```
-d <delimiter>
```

```
-b <byte o rango de byte> # -b 5 = extrae el 5º byte
```

```
-c <carácter o rango de car.> # Igual que byte
```

```
-f <field list>
```

```
<field list>:
```

```
    N (Nth byte),
```

```
    N- (From Nth byte to EOL),
```

```
    -N (from init to Nth byte),
```

```
    M-N (from Mth to Nth bytes)
```

```
# Ex: -f 5- = Desde 5º campo delimitado hasta final de línea
```

Corta una línea extrayendo la información especificada con las opciones.

- `awk [OPTIONS] '[condición] {comandos}'`

Intérprete de comandos de lenguaje AWK

Guía del Proyecto Born2beroot

[OPTIONS]

-F <field separator>
-f <program file>
-v var=value # Inicializa variable 'var' para BEGIN

[condición] que deben reunir las líneas o parámetros

Comandos:

\$0 Línea completa
\$1-\$N Campos (columnas) de línea
FS Separador (por defecto, espacio o TAB)
NR Número de línea (Ej: NR>1; NR==2)
OFS Output Field separator (defecto ' ')
ORS Output Record separator (líneas) (defecto '\n')
RS Input Record separator ('\n')
BEGIN Sentencias a ejecutar antes de procesado
END Sentencias a ejecutar después de procesado
length Longitud de línea en proceso
FILENAME Archivo en procesamiento
ARGC, ARGV N° parámetros, parámetros de entrada

Funciones (extracto):

close (file)
Funciones matemáticas
length(string)
print Impresión sin formato
printf Impresión con formato (Ej: printf "i= %d", i)

Operaciones con cadenas:

/<string>/ Búsqueda de cadena <string>
/^<string>/ Cadena al principio de línea
/<string\$/ Cadena al final de línea
\$N~/<string>/ Cadena en el campo N
\$N!~/<string>/ Cadena no en el campo N
/<string1>|<string2>/ OR
/<string1>/, /<string2>/ Líneas entre cadenas

Separador de comandos: ";" (punto y coma)

- wc [OPTION] [FILE]

Contar palabras, líneas o bytes

[OPTION]

-c Cuenta bytes
-m Cuenta caracteres

Guía del Proyecto Born2beroot

```
-l    Cuenta nuevas líneas
-w    Cuenta palabras
```

- Variables en archivos 'bash'

Declaración de variable: `var = value`

Asignación de operación a variable: `var = $(comandos/operaciones)`

Uso de variable: `var3 = $($var1 + $var2)`

Condición: `if [condition]; then Command(s); fi`

- Añadir tarea en 'crontab' con permiso para 'root':

```
sudo crontab -u root -e
```

Se abrirá editor con la tabla 'crotab' donde se añadirá la programación:

```
*/10 * * * * /usr/local/bin/monitoring.sh
```

NOTA: */10 = Ejecutar cada 10 minutos

- El 'script' que ejecutará 'cron' se colocará en:

```
/usr/local/sbin
```

Introducción a tareas programadas

'**cron**' es un administrador de procesos (scripts) en segundo plano (daemon), ejecutándolos periódicamente según estén programados en la tabla '**crontab**'

La estructura de la tabla '**crontab**'

```
* * * * * <user> <script.sh>
| | | | |
| | | | |_____ Día de la semana (0 - 6) (0 = domingo)
| | | | _____ Mes (1 - 12)
| | | _____ Día del mes (1 - 31)
| | _____ Hora (0 - 23)
| _____ Minuto (0 - 59)
```

Para la indicación de la fecha y hora, se pueden utilizar palabras reservadas:

```
@reboot    Ejecutar al inicio
```

```
@yearly    Una vez al año (0 0 0 0 *) # También @annually
```

```
@monthly    Una vez al mes (0 0 0 * *)
```

Guía del Proyecto Born2beroot

```
@weekly    Una vez a la semana (0 0 * * 0)
@daily     Una vez al día (0 0 * * *) # Igual que @midnight
@hourly    Una vez por hora (m * * * *)
```

Fuentes de datos para el script

- Arquitectura del sistema operativo y versión del kernel

```
uname [OPTIONS]
-o    Operating system
-s    Kernel system
-v    Kernel version
-r    Kernel release
-n    Network node hostname
-m    Machine hardware name
-a    (= uname -s -n -r -v -m -o)
```

- Número de procesadores físicos

```
/proc/cpuinfo      Línea "cpu cores"
```

- Número de procesadores virtuales

```
/proc/cpuinfo      Contar líneas "processor"
```

NOTA: 'cpuinfo' contiene un bloque de información para cada hilo de procesamiento

- Memoria RAM disponible y porcentaje de utilización

```
free -h    # Devuelve en formato humano (B, Ki, Mi, Gi):
            total used free shared      buff/cache available
Mem: xxx   yyz   zzz   ppp           qqz           rrr
Swap: xxx'  yyz'  zzz'
```

- Memoria disponible y porcentaje de utilización

```
free      # Sumar datos de Mem y Swap
```

- Uso de disco

```
df -BG     # Información de almacenamiento, en Gi
Sumar los datos de las particiones en /dev/
```

- Porcentaje de uso de núcleos

```
top -b -n 1 | grep '%CPU'
```

Guía del Proyecto Born2beroot

Extraer el cuarto campo (idle), utilizando ',' como delimitador y restarlo a 100%.
Parámetros: '-b' (modo batch, no envía respuesta hasta completar iteraciones); '-n' (número de iteraciones)

- Fecha y hora de último reinicio

```
who -b
```

- Estado de LVM (activo o no)

```
lsblk      # Devuelve los discos y particiones del sistema
```

Uno de los campos de la respuesta es el tipo de bloque, y los gestionados por LVM mostrarán este tipo. Se contarán las líneas que contienen 'lvm' para comprobar != 0

- Número de conexiones activas

```
/proc/net/sockstat      # Muestra tipo y número de sockets
```

Comprobar fila 'TCP' y número de sockets 'inuse'

- Número de usuarios usando el servidor

```
users      # Devuelve los usuarios 'logged'
```

Contar número de palabras: `wc -w`

- Dirección IPv4 y MAC del servidore

```
hostname -I      # Host network addr., except IPv6 & link local  
ip link          # Leer MAC de línea link/ether
```

NOTA: 192.168.56.1 es la dirección del adaptador host-guest de Virtualbox en el lado del host.

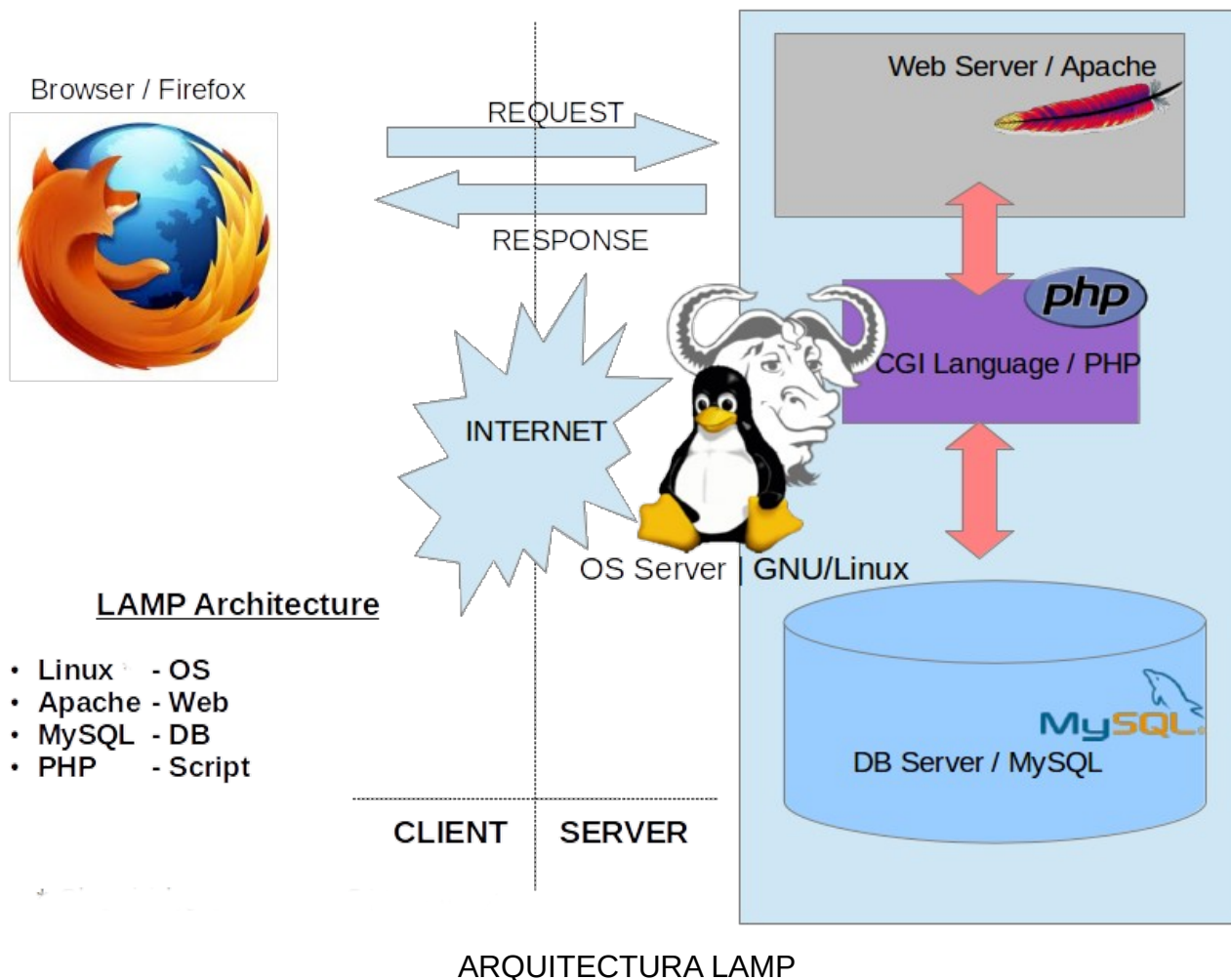
- Número de comandos ejecutados con 'sudo'

```
/var/log/auth.log  # Registra actividades con autenticación
```

Contar líneas que contienen 'sudo' en quinto campo con delimitador espacio.

3. Instalar servidor HTTP

3.1. Sistema de gestión de Web



3.2. Instalación y configuración de servidor HTTP

a) Instalar servidor HTTP y gestor de base de datos

```
sudo apt update
sudo apt install lighttpd
```

b) Configuración de 'lighttpd'

```
dpkg -l | grep lighttpd # Comprobar instalación correcta
sudo systemctl [start|stop] lighttpd #Iniciar/parar servicio
sudo systemctl status lighttpd
sudo ufw allow 80 # Abrir puerto 80 de HTTP en firewall
```

NOTA: Según la descripción en su página web, 'lighttpd' usa la memoria, CPU y otros recursos más eficientemente que otros servidores web.

3.3. Instalación y configuración de gestor de base de datos

a) Instalar gestor de base de datos mariadb-server

```
sudo apt install mariadb-server
dpkg -l | grep mariadb-server
sudo systemctl status mariadb
```

NOTA: MariaDB es un sistema de gestión de base de datos (SGBD) derivado de MySQL, desarrollado con el objetivo de mantener una versión de este con versión GPL. MariaDB reemplaza su correspondiente versión de MySQL, con algunas diferencias internas, pero manteniendo la compatibilidad de órdenes, interfaces, API y bibliotecas.

b) Configuración de MariaDB

```
sudo mysql_secure_installation
```

Responder al siguiente cuestionario (el mismo explica el significado de las preguntas):

```
Enter current password for root (enter for none): *****
Switch to unix_socket authentication [Y/n] n
Change the root password? [Y/n] n
Remove anonymous users? [Y/n] y
Disallow root login remotely? [Y/n] y
Remove test database and access to it? [Y/n] y
Reload privilege tables now? [Y/n] y
```

A partir de este momento para manipular el gestor de bases de datos deberá usarse permisos de 'sudo' para el usuario que ejecutó la instrucción anterior (en mi caso el usuario 'davidrod')

c) Crear base de datos

```
sudo mariadb
MariaDB[(none)]> CREATE DATABASE wpdb;
MariaDB[(none)]> GRANT ALL ON wpdb.* TO
'davidrod'@'localhost' IDENTIFIED BY '*****' WITH GRANT OPTION;
MariaDB[(none)]> FLUSH PRIVILEGES;
MariaDB[(none)]> SHOW DATABASES;
MariaDB[(none)]> exit
```

Comandos SQL usados:

CREATE DATABASE	(se explica por sí mismo)
GRANT	Provisión de privilegios

Guía del Proyecto Born2beroot

ALL	Todos los privilegios (EXECUTE, SELECT, DELETE, INSERT... Dependien de objeto)
ON <DB object>	Objetos: TABLE, VIEW, PROCEDURE...
TO <user>@<net>	
WITH GRANT OPTION	Permite que el usuario pueda dar los mismos privilegios sobre el objeto a otros usuarios
FLUSH <DB object>	Limpia la caché del objeto (en nuestro caso los privilegios del usuario)

Para acceder al gestor, con un determinado usuario:

```
mariadb -u davidrod -p
```

Pedirá contraseña. También se puede acceder con privilegio de 'sudo'.

3.4. Instalación de interprete de PHP

```
sudo apt install php-cgi php-mysql  
dpkg -l | grep php
```

3.5. Instalación de CMS WordPress

Instalar gestor de descargas 'wget'

```
sudo apt install wgetclear
```

Descargar WordPress

```
sudo wget http://wordpress.org/latest.tar.gz -P /var/www/html
```

Descomprimir CMS e instalar en carpeta raíz del servidor web

```
sudo tar -xzf /var/www/html/latest.tar.gz  
sudo rm /var/www/html/latest.tar.gz  
sudo cp -r /var/www/html/wordpress/* /var/www/html  
sudo rm -rf /var/www/html/wordpress
```

Configurar WordPress. Renombrar 'wp-config-sample.php' a 'wp-config.php'


```
23 define( 'DB_NAME', 'wpdb' );  
26 define( 'DB_USER', 'davidrod' );  
29 define( 'DB_PASSWORD', '<contraseña>' );
```

Configurar Lighttpd

```
sudo lighty-enable-mod fastcgi  
sudo lighty-enable-mod fastcgi-php  
sudo service lighttpd force-reload
```

Guía del Proyecto Born2beroot

Acceder a la instalación de WordPress introduciendo la dirección IP del servidor (Ej: **http://192.168.0.27**). Se mostrará la ventana de configuración de WordPress:



Welcome to WordPress. Before getting started, we need some information on the database. You will need to know the following items before proceeding.

1. Database name
2. Database username
3. Database password
4. Database host
5. Table prefix (if you want to run more than one WordPress in a single database)

We're going to use this information to create a `wp-config.php` file. **If for any reason this automatic file creation doesn't work, don't worry. All this does is fill in the database information to a configuration file. You may also simply open `wp-config-sample.php` in a text editor, fill in your information, and save it as `wp-config.php`.** Need more help? [We got it.](#)

In all likelihood, these items were supplied to you by your web host. If you don't have this information, then you will need to contact them before you can continue. If you're all ready...

Let's go!

Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	<input type="text" value="wpdb"/>	The name of the database you want to use with WordPress.
Username	<input type="text" value="davidrod"/>	Your database username.
Password	<input type="text" value="password"/>	Your database password.
Database Host	<input type="text" value="localhost"/>	You should be able to get this info from your web host, if <code>localhost</code> doesn't work.
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.

Submit

Guía del Proyecto Born2beroot

El nombre de la base de datos, usuario y contraseña son los creados el apartado 3.3.c)

Si no se modificó el archivo de configuración wp-config.php, mostrará un mensaje con el contenido del mismo, con los campos modificados, e instando a crearlo.

Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title

42 Málaga

Username

davidrod

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password

Vptyeopfa22I#V^PEG

Hide

Strong

Important: You will need this password to log in. Please store it in a secure location.

Your Email

Double-check your email address before continuing.

Search engine visibility

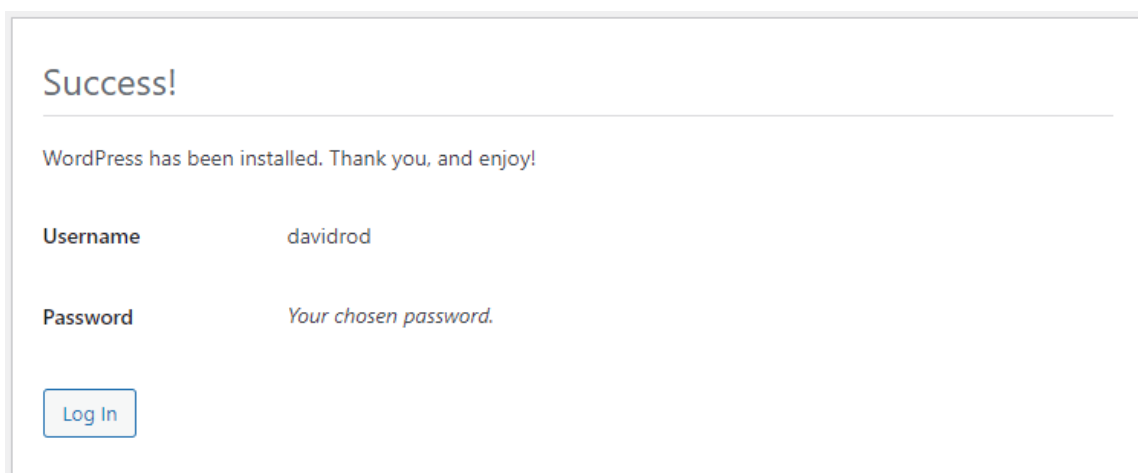
☒ Discourage search engines from indexing this site

It is up to search engines to honor this request.

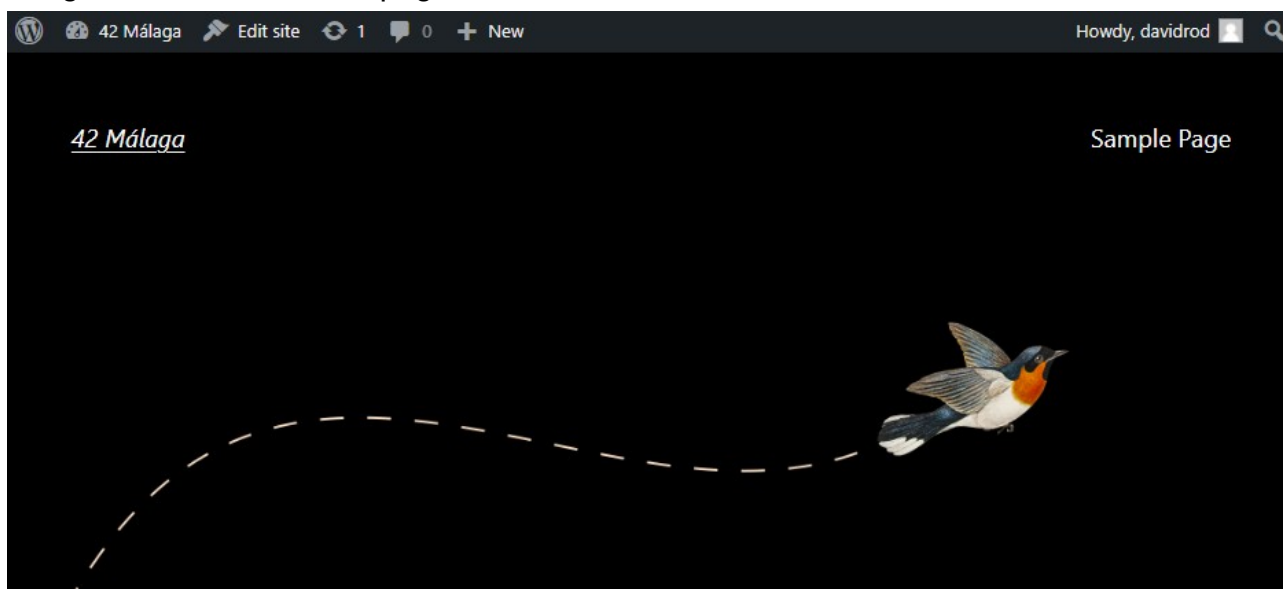
Install WordPress

Es obligatorio incluir una dirección de 'email' que puede ser inventada.

Guía del Proyecto Born2beroot



A partir de este momento, la introducción de la dirección IP del servidor desde un navegador web abrirá esta página.



Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

May 13, 2022

Para configurar la página se realiza 'login' en la siguiente dirección:

`http://192.168.0.27/wp-admin/`

4. Instalar servidor FTP

4.1. Instalación y configuración

- Instalar vsftpd
`sudo apt install vsftpd`
- Comprobar la correcta instalación
`dpkg -l | grep vsftpd`
`dpkg -l` Listar los paquetes instalados
- Añadir puerto 21 a UFW
`sudo ufw allow 21`
- Configurar 'vsftpd'
`sudo vim /etc/vsftpd.conf`

Parámetros:

```
anonymous_enable = YES
write_enable = YES # Allow upload files via ftp
chroot_local_user = YES # Restrict users to their /home
allow_writeable_chroot = YES # Añadir al archivo
```

NOTA: Se creará la siguiente estructura de directorios para usuario:

/home/<usuario>/ftp/files con los siguientes permisos:

```
sudo chown nobody:nogroup /home/<user>/ftp
sudo chmod a-w /home/<user>/ftp
```

Se añadirán las siguientes líneas al archivo /etc/vsftpd.conf:

```
user_sub_token=$USER
local_root=/home/$USER/ftp

userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

Y se descomenta la línea 114: `chroot_local_user=YES`

- Reiniciar 'vsftpd'
`sudo service vsftpd restart`
`systemctl status vsftpd.service`
- Crear, si no existe, el archivo: /etc/vsftpd.userlist y añadir los usuarios con permiso para hacer 'ftp'.

4.2. Transferencia de archivos vía FTP

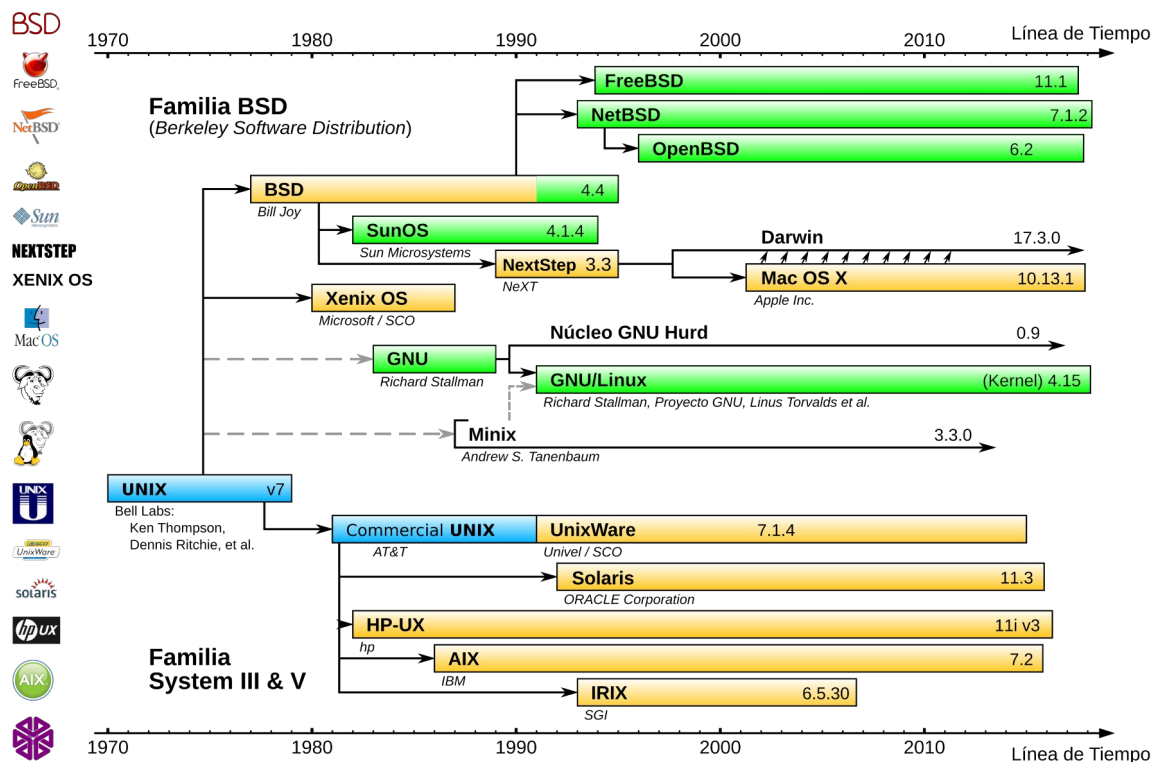
- **Conexión FTP**
`ftp <ip address>`

Pedirá usuario y contraseña en el servidor
- **Enviar archivo**
`send <local_file> [<remote_file>]`
- **Recibir archivo**
`lcd <local_directory>`
`get <remote_file>`
- **Desconexión**
`ftp> quit`

5. Fundamentos teóricos

5.1. Sistemas basados en UNIX

Evolución de los sistemas UNIX y estructura del sistema Linux



Modo de usuario	Aplicaciones de usuario	Por ejemplo, <code>bash</code> , LibreOffice, GIMP, Blender, 0 A.D., Mozilla Firefox, etc.				
	Componentes del sistema de bajo nivel::	Demonios del sistema: <i>systemd, runit, logind, networkd, PulseAudio, ...</i>	Sistema de ventanas: <i>X11, Wayland, SurfaceFlinger (Android)</i>	Otras bibliotecas: <i>GTK+, Qt, EFL, SDL, SFML, FLTK, GNUstep, etc.</i>	Graficos: <i>Mesa, AMD Catalyst, ...</i>	
	Biblioteca estándar de C	<code>open()</code> , <code>exec()</code> , <code>sbrk()</code> , <code>socket()</code> , <code>fopen()</code> , <code>calloc()</code> , ... (hasta 2000 subrutinas) <i>glibc</i> pretende ser rápido, <i>musl</i> y <i>uClibc</i> sistemas embebidos, <i>bionic</i> escrito para Android, etc. Todos pretenden ser compatibles con POSIX/SUS .				
Modo de Núcleo	Núcleo Linux	<code>stat</code> , <code>splice</code> , <code>dup</code> , <code>read</code> , <code>open</code> , <code>ioctl</code> , <code>write</code> , <code>mmap</code> , <code>close</code> , <code>exit</code> , etc. (alrededor de 380 llamadas al sistema) La interfaz de llamada al sistema del núcleo Linux (SCI, tiene como objetivo ser compatible con POSIX/SUS)				
		Subsistema de planificador	Subsistema de IPC	Subsistema de gestión de memoria	Subsistema de archivos virtuales	Subsistema de red
		Otros componentes: ALSA , DRI , evdev , LVM , device mapper , Linux Network Scheduler , Netfilter Linux Security Modules : <i>SELinux, TOMOYO, AppArmor, Smack</i>				
Hardware (CPU, memoria principal, dispositivos de almacenamiento de datos, etc.)						

5.2. Comparativas

Comparación Centos vs Debian

Fuente: <https://1gbits.com/blog/debian-vs-centos/>

Parameters	CentOS	Debian
Community	Supported by the Red Hat community	Supported by Debian individuals
Market Presence	CentOS has a large market due to its user-friendly nature	Debian lacks market presence due to its terminal end usage
Architecture Support	CentOS does not come with multiple architecture support	Debian has multiple architecture support as compared to other distributions
Release Cycle	New updates and upgrades usually take time , thus making it stable	It has a release cycle of 2 years , thus giving it enough time to fix bugs
Version Upgrade	It is better to install a new CentOS version rather than go for upgrading the older version. This task is cumbersome	Debian can be easily upgraded from one stable version to another
User Interface	CentOS has a complicated GUI	Debian comes with user-friendly applications and GUI
Package Manager	CentOS uses YUM as its package manager	Debian uses apt-get as its package manager
Package Number	CentOS has limited packages	Debian has a vast amount of packages in its default repository

Comparación SELinux vs AppArmor

Fuente: <https://es.wikipedia.org/wiki/SELinux>

SELinux	AppArmor
Orientado a objetos (archivos, redes...)	Orientado a sistema de archivos
Política centrada en objetos A cada objeto se le asigna una etiqueta (contexto de seguridad) de determinará el acceso a este	Política centrada en las tareas Control de accesos basado en rutras
Denegación por defecto en todo caso	Denegación por defecto aplica solo a las tareas que controla
Control más fino	Más fácil de configurar

Comparación 'aptitude' vs 'apt' vs 'apt-get'

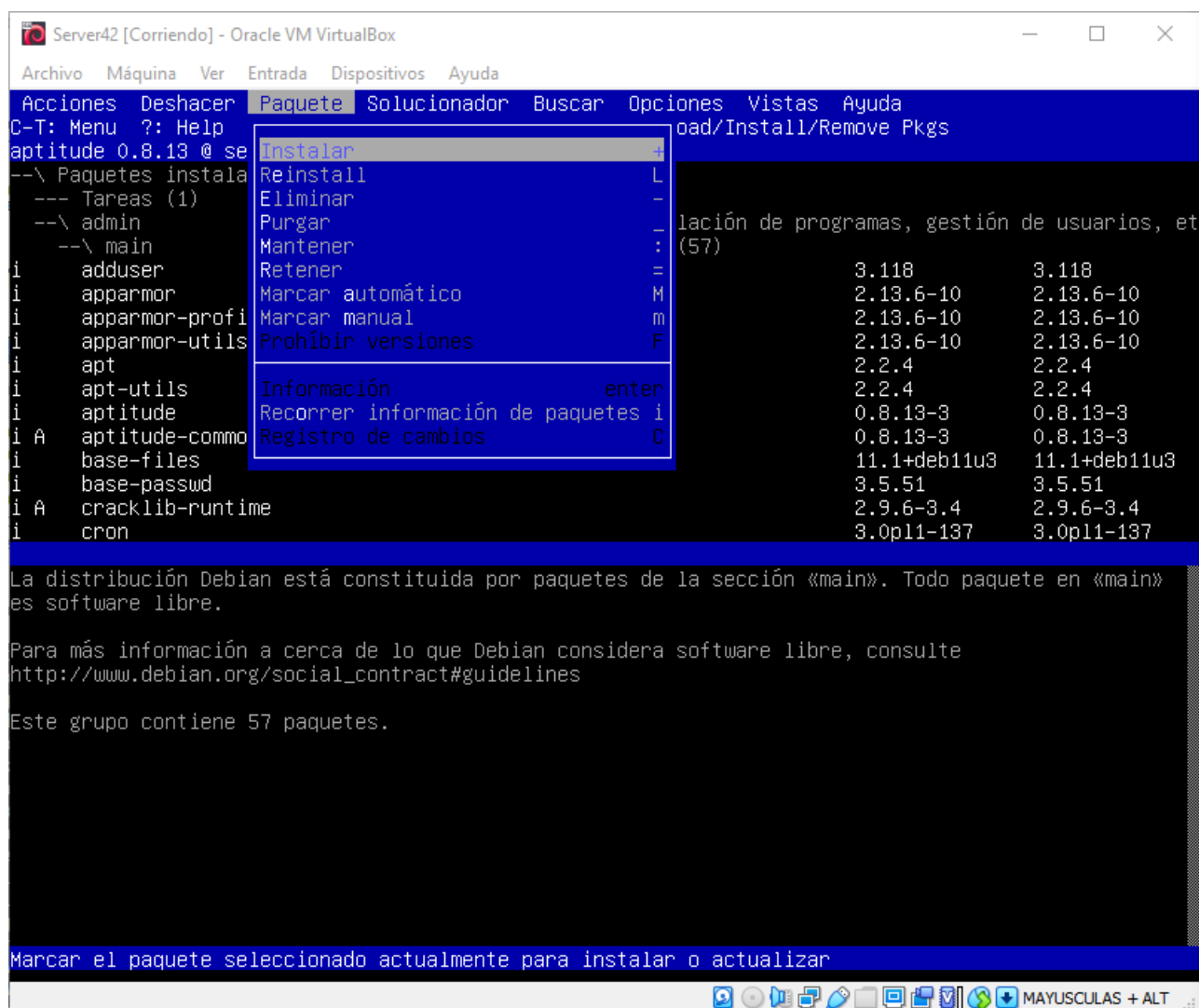
Fuente: <https://juncotic.com/apt-vs-apt-get-vs-aptitude-algunas-notas/>

En distros basadas en Debian, el gestor de paquetes estándar es 'dpkg'. Los paquetes pueden tener dependencias, otros paquetes que deben ser previamente instalados. Estas dependencias se gestionan mediante APT (Advanced Package Tool) que tiene diferentes 'frontends':

- a) En modo comando: apt-get, apt-cache, apt-mark
- b) En modo gráfico: Synaptic, Ubuntu Software Center...
- c) En modo comando y gráfico con texto: aptitude

'apt' combina las funcionalidades de apt-get y apt-cache

'aptitude' combina funcionalidades de apt-get, apt-cache y apt-mark. La diferencia más llamativa con 'apt' y 'apt-get' es que tiene un interfaz gráfico en modo texto (como 'nano' o los programas de ordenador antes de la era Windows).



En la imagen anterior 'aptitude' ejecutándose. De instalarse mediante apt o apt-get. Para ejecutarlo en modo interactivo gráfico, se ejecuta: 'aptitude'. En modo comando funciona igual que 'apt'.

NOTA: Para acceder al menú se pulsa: CTRL+T

Además, estos dos 'frontends' incluyen algunas funcionalidades propias.

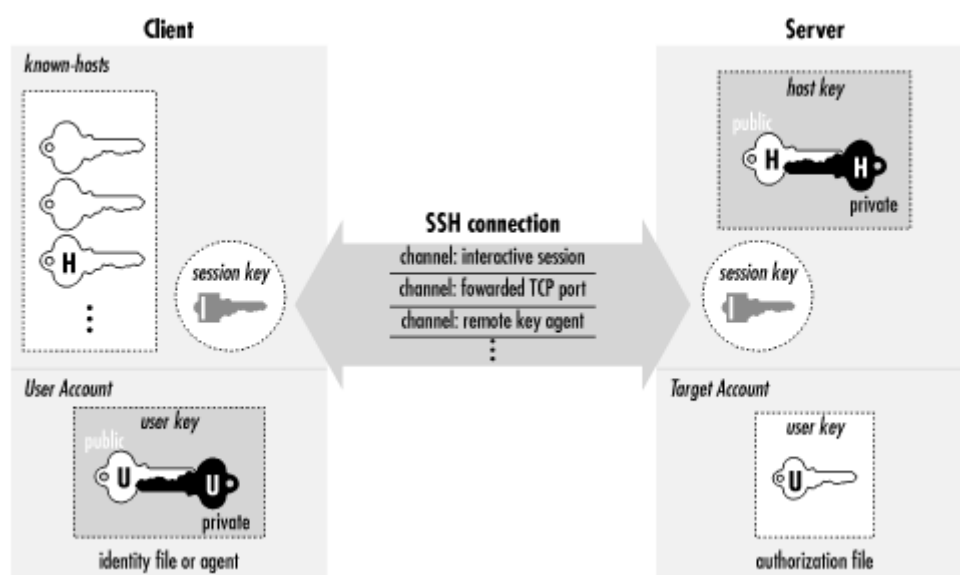
5.3. Volúmenes encriptados y SSH

El uso de un volumen encriptado lo protege del acceso a sus datos en caso de pérdida o robo del almacenamiento.

Es aconsejable crear contraseñas de respaldo para solventar la posibilidad de olvido de la contraseña inicial. Ver siguiente [enlace](#).

Mediante el protocolo SSH se establece un canal seguro entre un servidor y equipos remotos.

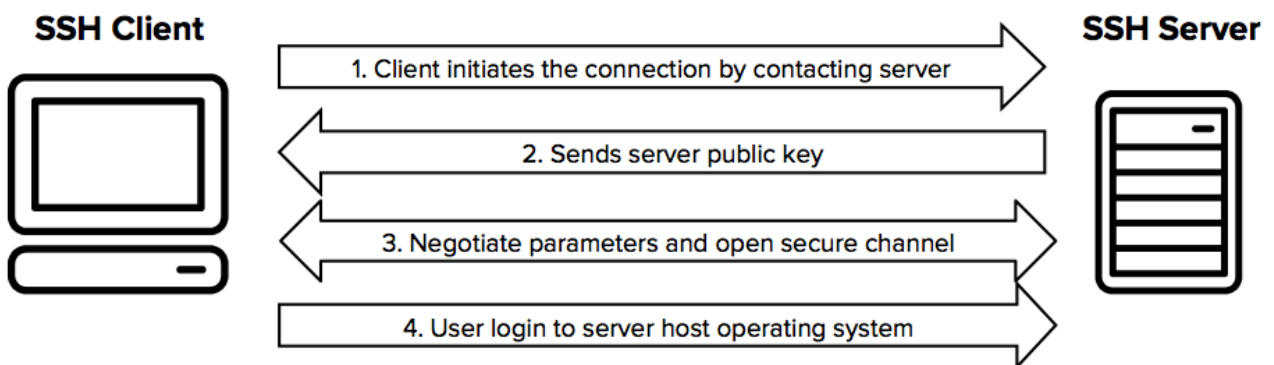
Fuente: https://docstore.mik.ua/oreilly/networking_2ndEd/ssh/index.htm



Cada lado de la conexión protege su clave privada (en negro) y comparte su clave pública (en blanco). Si el cliente quiere enviar un mensaje encriptado al servidor, lo cifra con la clave pública del servidor. Para descifrar el mensaje, el servidor utiliza su clave privada.



Esquema de cifrado con clave pública

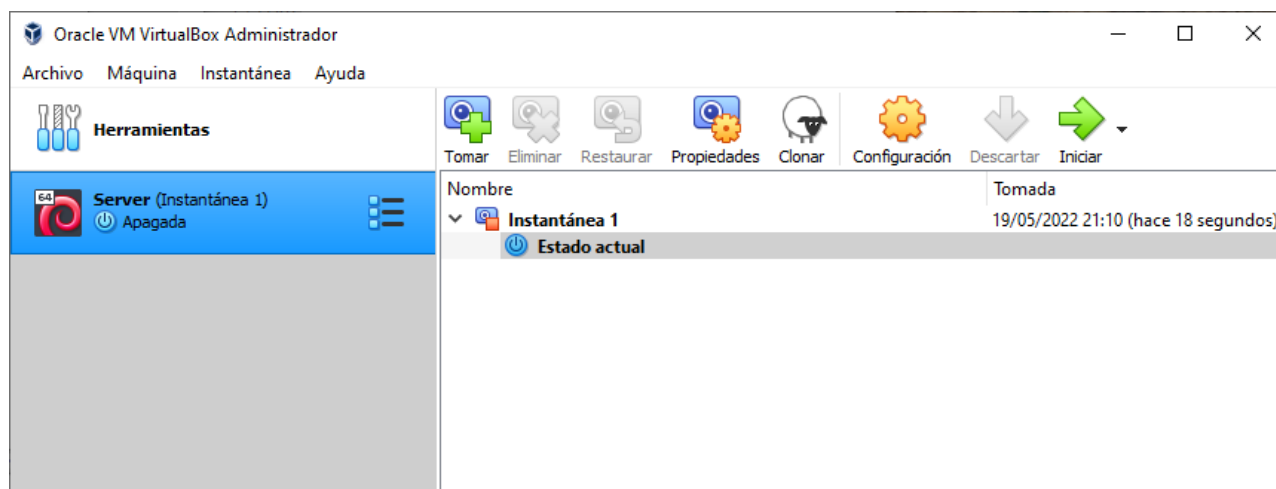


Esquema de establecimiento de conexión segura

6. Entrega de proyecto

Tras tener configurado el servidor con los requerimientos del proyecto, se apagará y se tomará una instantánea de la máquina virtual. Después, y antes de volver a arrancar la máquina, se creará la suma 'hash' que identifica su estado y que será la firma que hay que subir al repositorio del proyecto.

Para crear la instantánea, o 'snapshot', se abren las herramientas en Virtualbox y se 'toma' la instantánea (botón "Tomar" o "Take") teniendo seleccionada la máquina virtual.



Para calcular la firma de la máquina virtual se utiliza el comando:

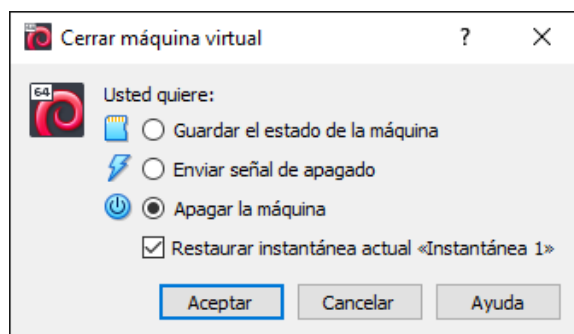
```
sudo shasum <server_virtual_disk>.vdi
```

```
davidrf@DESKTOP-DAVIDRF:/mnt/c/Users/david/VirtualBox VMs/Server$ sudo shasum Server.vdi
239909e1d42ed901f4ec20f7f36de8b71de1b41a  Server.vdi
davidrf@DESKTOP-DAVIDRF:/mnt/c/Users/david/VirtualBox VMs/Server$
```

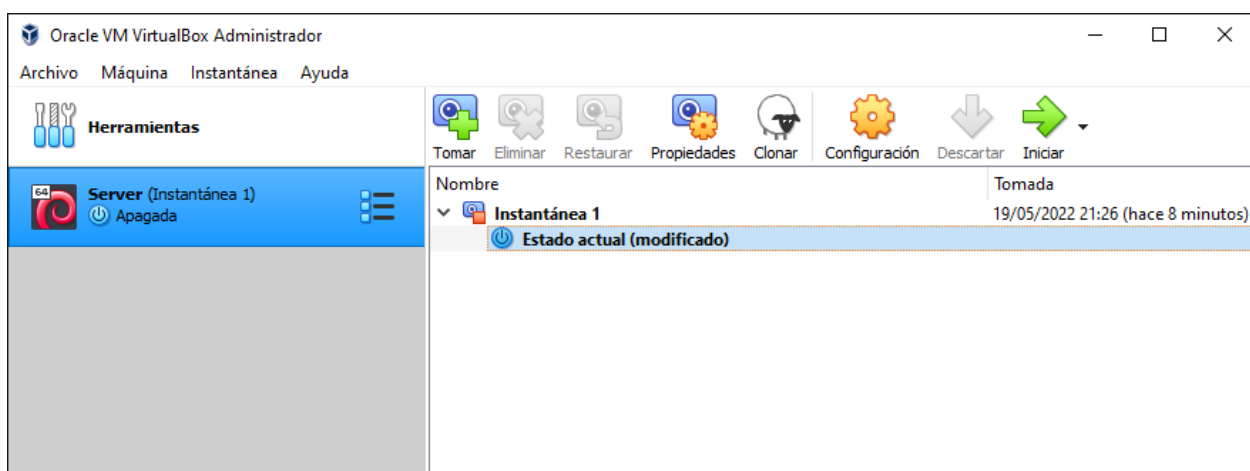
Guardar la suma 'hash' (copy/paste) en el archivo 'signature.txt'

Cuando se vuelva a ejecutar la máquina virtual en el examen, se producirán modificaciones. Para no guardar dichos cambios y, por tanto, no variar la suma 'hash' (que no coincidiría con el guardado en 'signature.txt') cerrar la máquina (en botón de cierre de ventana, no con 'shutdown') con la siguiente opción de 'Restaurar instantánea...':

Guía del Proyecto Born2beroot



Si por algún motivo se olvidara marcar la opción "Restaurar instantánea...", el estado actual estará modificado



En ese caso, se seleccionará la instantánea tomada para obtener la firma entregada, y se pulsará "Restaurar", **desmarcando** "Crear una instantánea del estado actual" (que generaría "Instantánea 2"). Esto recuperará el estado de la máquina a la "Instantánea 1".

