

# Practica1 Virtualizaci3n e instalaci3n de...



**BetaNT82**



**Ingeniería de Servidores**



**3º Grado en Ingeniería Informática**



**Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación  
Universidad de Granada**

**Aprende Inglés**  
Con nuestros cursos **GRATUITOS**  
para desempleados

**Pincha aquí e  
inscríbete ya**

**Fórmate con nuestros cursos de Inglés para las titulaciones  
A1, A2, B1 y B2 100€ subvencionados para desempleados**



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE TRABAJO  
Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO  
DE EMPLEO ESTATAL  
**SEPE**



# Aprende Inglés

Con nuestros cursos **GRATUITOS**  
para desempleados



**Fórmate con nuestros cursos de Inglés para las titulaciones  
A1, A2, B1 y B2 100€ subvencionados para desempleados**

**Pincha aquí e  
inscríbete ya**

**958 047 283  
621 21 76 50**



Aprende **Inglés**

Con nuestros cursos **GRATUITOS**  
para desempleados



MINISTERIO  
DE TRABAJO  
Y ECONOMÍA SOCIAL



Junta de Andalucía  
Consejería de Empleo, Formación  
y Trabajo Autónomo



Fórmate con nuestros cursos de Inglés para las titulaciones  
A1 B1 A2 y B2 100% subvencionados para desempleados

Pincha aquí e  
inscríbete ya

958 047 283  
621 21 76 50

# Practica 1: Virtualización e instalación de SO's

## 1. Introducción

Trabajar con servidores es costoso que se consiga por el VPS (Virtual Private Server) está más estandarizado. A esto se le debe añadir que el concepto de Housing está aumentando.

El housing es comprar el servidor y pagar un servicio para que lo guarden en físico y se encarguen de mantenerlo y darle un cuidado físicamente pero el administrador eres tú o otra persona si la has encontrado para ello.

Estas prácticas están bien pero se pueden tener problemas con la protección de datos, para ello se hace un manejo híbrido, teniendo datos en la nube y datos en local. Las leyes que regulan esto son la RGPD (2015) y su versión española LOPD (2018). Tiene mucho detalle, hasta tal punto de que las prácticas que realizamos la incumplimos.

### 1.1 Software para virtualización

Virtualbox perteneciente a Oracle.

## 2. Software para servidores

Una de las distribuciones mejores para servidores es RHEL (Red Hat Enterprise Linux). Con esta distribución esta relacionada Fedora, mantenida por la comunidad y con soporte de Red Hat, se podría decir que es una beta de Red Hat. Cuando se optimiza Fedora se incorpora a Red Hat.

Cuando RedHat terminaba de hacer sus paquetes CentOS realizaba su versión y la subía sin ninguna empresa o logo, ya que es desarrollada por la comunidad. Pero con el tiempo RedHat financió a CentOS por lo que se ha convertido en RedHat sin soporte y sin documentación

Luego tenemos Debian, que desarrolla Ubuntu y es la que vamos a ver con más desarrollo en las prácticas.

Además de estos software para servidores tenemos otros como Solaris, (Free)BSD, Windows-Server, etc.

## Ejercicio 1

### Conocimientos sobre la práctica

CMS (Content Management System).

La configuración que se suele aplicar para un CMS es un RAID1 con LVM. Además se hacen 3 volúmenes lógicos y una partición para el arranque.

### Ventajas y desventajas del tipo de espacio.

Si reservamos memoria de forma dinámica, vamos a tener menos problemas con el espacio, como que sobre espacio o realizar transferencias. Pero por otro lado no vamos a poder aprovechar la localidad espacial y vamos a tener fragmentación en la memoria.

### RAID

Es un acrónimo de Redundant Array (originariamente inexpensive, pero actualmente:) Independent Disks. Esto significa que tenemos una matriz de discos.

Si el RAID es de tipo 0 usamos la matriz de disco para aumentar la velocidad, dividiendo la información entre los discos y realizando lecturas en paralelo al recuperarlo.

Si el RAID es de tipo 1 usamos la matriz de disco para tener la seguridad, teniendo la misma información en todos los discos.

Se puede fusionar los dos tipos de RAID para tener RAID 1+0 y tener ambas ventajas o para comprobar la paridad y obtener nuevos tipos de RAID. El raid se puede hacer a través de Hardware o de Software.

La capacidad del RAID será la capacidad del disco más pequeño, Más adelante veremos como utilizar el espacio sobrante para tener la información duplicada.

## Particiones

El disco se puede dividir lógicamente en distintas particiones. Al crear una nueva partición del disco se crea otra partición para el BIOS grub. Esta partición nueva es de tamaño pequeño y es solo para instalar el grub, este se usará en el Master Boot Recorder, esto se hace porque si no aparece en el grub no podremos iniciar nada en ese disco.

Si vamos a usar las particiones para un raid debemos dejarlas sin formato.

## LVM

A partir de las particiones podemos crear otra abstracción superior llamados physical volume, estos van mapeados sobre las particiones.

Estos physical volume se agrupan en volume group, estos grupos hacen referencia tanto a volúmenes físicos como a lógicos. Con esto nos referimos a que un conjunto de volúmenes físicos los podemos presentar como otro de volúmenes lógicos (no tienen porque ser 1 a 1 los volúmenes, podemos tener 3 volúmenes de tamaño x físicos y que estos resulten en 5 volúmenes lógicos de tamaño y). A esta estructura que se forma es lo que llamamos LVM (logical volume management).

Esto se puede usar para hacer snapshots, capturas de los volúmenes para tener una copia de seguridad y nos da mayor flexibilidad.

Un ejemplo práctico es que si tenemos un disco físico que se corresponde con un volumen lógico, si añadimos otro disco físico con LVM podemos hacer que solo haya un volumen lógico.

## Que tamaño darle a la partición

Lo más cómodo es seguir la documentación. En casa de no tenerla a mano debemos realizar un análisis. Para ello vamos a analizar este ejemplo.

Nuestro LVM va a tener dos imágenes encriptadas, como van a estar encriptadas a /boot tenemos que asignarle un espacio a esta partición. El tamaño dependerá del kernel de Linux, pero no pasara de las decenas de megas, por lo que le asignaremos 150 megas que será un máximo. Como mínimo queremos tener 2 imágenes coexistiendo, por ello le asignamos 300 megas en una partición independiente.

Los tamaños para root, swap y home, es darle la mayoría a root.

Swap es para realizar cambios que supondremos que no deberemos realizar muchos, por lo que dejarle 1G de 10G es buen tamaño.

Como nuestro ejemplo es un CMS en /home no le dejaremos muchos datos, por lo que un tamaño pequeño es correcto.

## Procedimientos

1. Creamos máquina de virtual box
2. Seleccionamos la memoria. Para ello miramos la indicada, si no se ha indicado se mira en la documentación. Asignamos 1GB en este caso.
3. Seleccionamos espacio, para ello creamos un disco virtual
4. En configuración/almacenamiento añadimos otro disco, es decir, añadimos otro controlador SATA.
5. Añadimos el cd con la imagen de Ubuntu-Server y seleccionamos cd vivo.
6. Iniciamos la máquina, los pasos actuales se realizarán dentro de la máquina virtual.
7. Seleccionamos idioma español, continuar sin actualizar y configuramos el teclado. Las conexiones de red las marca automáticamente. No es necesario especificar el proxy. El mirror dejamos el de ubuntu.
8. Seleccionamos Custom Storage layout
9. Sobre el VDISK que se encuentra como dispositivo de arranque y creamos una partición de 300M sin formato.
10. Seleccionamos el otro disco como otro dispositivo de arranque (select as another boot device)
11. Realizamos una partición igual a la que hicimos antes en este nuevo disco
12. Entramos en el apartado create software raid (md). El md es de multidivice.
13. Seleccionamos las dos particiones y lo creamos, tendrá el nombre md0.
14. En los dos discos creamos particiones sin formato y sin especificar el tamaño (esto hace que seleccione el tamaño entero).

# Aprende Inglés

## Con nuestros cursos **GRATUITOS** para desempleados



MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL



Junta de Andalucía  
Consejería de Empleo, Formación y Trabajo Autónomo



Fórmate con nuestros cursos de Inglés para las titulaciones  
A1 B1 A2 y B2 100% subvencionados para desempleados

Pincha aquí e  
inscríbete ya

958 047 283  
621 21 76 50

15. Creamos un nuevo RAID con estas dos particiones nuevas, tendrá el nombre md1.
16. Seleccionamos md0>format y aquí seleccionamos formato ext4 y montarlo sobre /boot.
17. Seleccionamos crear grupo de volúmenes y el dispositivo que marcamos es md1. Marcamos la opción de cifrado y ponemos la contraseña practicas,ISE. Este se llamara vg0
18. Seleccionamos vg0 y le damos a create Logical volume, y creamos lv-0-raiz con formato ext4 y lo montamos en / con 8G
19. Seleccionamos vg0/create Logical Volume, le asignamos 1G con formato swap
20. Seleccionamos vg0/create volume group con el resto del vg, con formato ext4 y en /home
21. Comprobamos si es correcto y le damos a hecho, si sale aviso de acción destructiva le damos a continuar
22. Rellenamos con nombre de usuario (nombre con iniciales de apellidos), nombre del servidor (que sea representativo como ubuntuISE20) y contraseña la misma que la anterior practicas,ISE. En un entorno real nunca se reciclan contraseñas.
23. Marcamos que no queremos instalar el servidor Openssh ni instalamos ningún otro recurso. Se inicia el proceso de instalación y cuando salga la opción de cancelar actualización la seleccionamos.
24. Al terminar de instalarse ejecutamos el comando lsblk para comprobar si se ha realizado bien la instalación.

## Ejercicio 2

### Conocimiento previo

#### XFS vs EXT4

XFS soporta metadata journaling que se basa en super bloques para la rápida recuperación de datos, que tiene el histórico de las diferentes operaciones, y ext4 tambien mete el journaling desde ext3.

Elegimos ext4 para CentOS tenemos la posibilidad de reducir el filesystem mientras que con xfs no se puede, aunque con Red Hat si se puede actualmente. Elegimos EXT4 para mayor flexibilidad.

## El mapper

En vez de usar la ruta específica podemos aplicar con `/dev/mapper/` podemos acceder al disco si no conocemos la ruta exacta ya que autocompletando (con `tab`) obtendremos la mayoría de los discos que queramos usar, para ver que no importa, usaremos en esta lección el mapper y en la siguiente solo usaremos la ruta relativa.

## Procedimiento

1. `lsblk` para comprobar que este todo bien
2. Pasar super usuario
3. `fdisk /dev/sdb` y marcamos opcion `m`(menu), opcion `n`(nueva partición), opcion `1`(tipo partición) y tamaño por defecto. Ponemos `w` antes de salir.
4. `lsblk` para comprobar que este bien hecha
5. Vemos los PV, y creamos uno nuevo sobre la partición con `pvccreate /dev/sdb1`.
6. Borramos la partición anterior con la opción `d`. Y creamos otra vez otra partición con `+6 G`, en caso de no caber `1.2 G` o `1,2 G`
7. Observamos con `pvs` los discos, y que si muestra menos es que hay espacio para metadatos.
8. Vemos el tamaño del VG con `vgdisplay`
9. Añadimos el disco al vg con `vgextend cl /dev/sdb1`. El tamaño final es los `6 G` nuevos más lo que había antes
10. Con `lvresize` añadimos espacio lógico, pero habría que reconfigurar el sistema de archivos.



11. Creamos otro disco lógico con `lvcreate -L3G -n new_var cl`. Con esto tenemos 3 logical volume y aun nos sobra espacio para aumentar el resto de discos
12. Creamos sistema de archivos `mkfs`
13. Creamos el directorio `new_var` y montamos el disco `mount /dev/mapper/cl-new_var /new_var`
14. Entramos con `systemctl isolate rescue`. Si no ejecutamos `systemctl status`
15. Ahora copiamos, por seguridad, con `cp -a /var/ /new_var/`
16. Por cada mount hay que hacer un `umount`, `umount /new_var`
17. Editamos el archivo `fstab` con `vi /etc/fstab`. Con G vamos al final, insertamos nueva linea y ponemos `/dev/mapper/cl-new-var /var xf defaults 0 0`. Entre cada apartado no hay espacios, hay tabuladores. Para salir le damos `esc` y escribimos `:wq`
18. Movemos la copia, `mv /var /var_old`
19. Restauramos `mkdir /var & restorecon /var & mount -a`. Mount -a hace que todos los filesystems se monten como estan indicados en `fstab`.

## Ejercicio 3

### Conocimiento previo de la práctica

Como configuración inicial encontramos dos particiones en `sda`. En la partición 2 encontramos nuestro PV, que se agrupa como VG y que está formado por dos LV, el `/` y el `SWAP`.

Nuestro nuevo PV(physical volume) no debemos extenderlo con CL, ya que el raid solo lo queremos para `/var`. Por ello debemos crear un nuevo VG(volume group) con su volumen lógico para `/var` cifrado.

Para cifrarlo podemos hacerlo con:

- Configurar el volumen lógico y luego cifrarlo (LUKS on LVM).
- Primero cifrarlos, y sobre el cifrado configurar los volúmenes (LVM on LUKS). Este lo realizamos en el ejercicio 1. Este permite realizar distinto cifrado a

cada volumen.

Obligatorio usar vi.

Nosotros tenemos /var cifrado, pero que pasa si se lleva a disco la página de memoria? que se lleva a SWAP información protegida sin proteger. Para que el caso este completo deberíamos cifrar swap tambien

## Tamaño de los discos

Al ser vídeos muy grandes, 2G sería inviable, pero por el hecho de que no tenemos esos discos físicamente usaremos 2G, para que no ocupe tanto espacio. Recordad que al ser un RAID 1, el tamaño del disco va a ser 2G, ya que en un RAID el tamaño máximo lo cogemos del menor.

Se podría usar el espacio sobrante del disco de 8G para tener la información duplicada en ese disco también y simular un RAID 1 con 3 discos.

## Orden mdadm

Es el diminutivo de multidivice administrator. Sirve para administrar dispositivos múltiples como los RAID.

Con el parametro - -level indicamos que tipo de raid queremos crear. Tenemos que indicar con cuantos dispositivos y donde están esos dispositivos. También debemos darle un nombre al dispositivo, en el paso 4 hay un ejemplo de como se invoca a esta orden.

## Nombres significativos

En la realización del ejercicio establecemos el nombre new\_var en el paso 7, y es un nombre que arrastramos durante toda la instalación. A la hora de asignar nombres a los volúmenes se les debe asignar nombres más significativos, el mejor nombre en este caso sería raid1 para remarcar que ese vg es el correspondiente al único raid que tenemos.

Al poner raid en el paso 9 pondríamos var RAID en el primer new\_var y en el segundo pondríamos raid1

## Orden cryptsetup

# Aprende Inglés



MINISTERIO  
DE TRABAJO  
Y ECONOMÍA SOCIAL



## Con nuestros cursos **GRATUITOS** para desempleados

Junta de Andalucía  
Consejería de Empleo, Formación  
y Trabajo Autónomo



Fórmate con nuestros cursos de Inglés para las titulaciones  
A1 B1 A2 y B2 100% subvencionados para desempleados

Pincha aquí e  
inscríbete ya

958 047 283  
621 21 76 50

Este comando se utiliza para realizar varias operaciones sobre archivos encriptados. Se pueden abrir, encriptar, formatear y demás.

luksOpen permite activar un dispositivo y le asigna un nombre.

Así para crear encriptaciones siempre deberemos formatear, activar, montar y después copiar la información, esta última se debe realizar de forma atómica.

### Shred

Para que no haya error de cifrado usamos shred, que sobrescribe un archivo para ocultar sus contenidos, es decir, que escribe basura. Para estar más seguro se realiza varias veces. Esto sigue un protocolo de protección de datos. En esta práctica supondremos que lo hemos ejecutado entre el paso 10 y 11.

### Activación automática de crypt

Para que se active automáticamente se indica en el archivo `/etc/crypttab`. En el archivo lo que tiene es el nombre (el mismo que en el mapper), el segundo tiene el camino relativo, el tercero es donde está alojada la clave. Lo que nos interesa es el UUID, este se puede encontrar con el comando `blkid` (se busca el que pone `crypto_LUKS` en el campo `type`), para verlo mejor hacemos `blkid | grep crypto`.

### ¿El cifrado está completo?

Nosotros tenemos `/var` cifrado, ¿pero que pasa si se lleva a disco la página de memoria? que se lleva a SWAP información protegida sin proteger. Para que el caso este completo deberíamos cifrar swap tambien

### Pasos a seguir

1. A la máquina virtual le añadimos dos discos por controlador SATA, teniendo así `sda`, `sdb`, `sdc`. En el ejemplo usaremos 8G y 2G, pero el tamaño no es significativo
2. Iniciamos la máquina y ejecutamos `lsblk` para comprobar que los discos están ahí.
3. Lo ideal sería que este paso fuese realizar una partición sobre los discos pero vamos a usar el disco entero.

4. Creamos el RAID 1 con `mdadm md0 - -create - -level=1 - -raid-devices=2 /dev/sdb /dev/sdc`
5. Con el `lsblk` vemos si se ha creado, en este caso se ha creado `md127`
6. Creamos un physical volumen con `pvcreate /dev/md127`
7. Creamos un nuevo volume group para new var sobre el raid. Se crea con `vgcreate new_var /dev/md127`
8. Comprobamos que esté bien con `vgdisplay`
9. Creamos el volumen logico con `lvcreate - n new_var -L 2G new_var`. En caso de que no quepa poner 1.9G
10. Comprobamos que este bien con `lvs`
11. Aplicamos `cryptsetup luksFormat /dev/new_var/new_var`. Escribimos YES para confirmar
12. Activamos el cifrado con `cryptsetup luksOpen /dev/new_var/new_var new_var_crypt`
13. Para asegurarnos de que está hacemos `ls /dev/mapper` y nos debería salir `new_var_crypt`
14. Creamos el directorio donde montar new\_var (`mkdir new_var`)
15. Creamos el sistema de archivos con `mkfs -t xfs /dev/mapper/new_var_crypt`
16. Montamos el sistema de archivos `mount /dev/mapper/new_var_crypt /new_var`. Ante la duda mostramos con `mount` los sistemas de archivos montados
17. Escribimos `system isolate rescue`, nos logeamos con root con la contraseña que le hallamos puesto al root.
18. `cp -a /var/. /new_var`
19. Editamos el fichero `/etc/fstab` con `vi` ( si queremos salir sin guardar usamos `:q!` ). En el fichero ponemos: `/dev/mapper/new_var-new_var_crypt /var xfs defaults 0 0`, recordad que todos son tabulados no espacios menos el que hay entre los ceros.



20. Vamos a crear la activación automática de nuestra encriptación. Para ello vamos a guardarlo en crypttab. Vemos primero que no haya nada en crypttab con `cat /etc/crypttab`
21. Guardamos el uuid con `blkid | grep crypto >> /etc/crypttab` (ponemos dos > para que no sobrescriba y añada al final)
22. Entramos al fichero y dejamos solo el nombre en este caso `new_var-new_var_crypt`, al uuid le quitamos las comillas y en el último campo ponemos `none`.
23. Movemos el `/var` con `mv /var /var_old`
24. Y restauramos `mkdir /var && restorecon /var`
25. Hacemos `reboot` para ver si nos hemos equivocado
26. Realizamos los pasos de cifrado esta vez con `swap` o desactivamos con `swapoff` el `swapping` para que el disco cifrado esté asegurado