# ISE
# PRACTICA 1

## Día 1

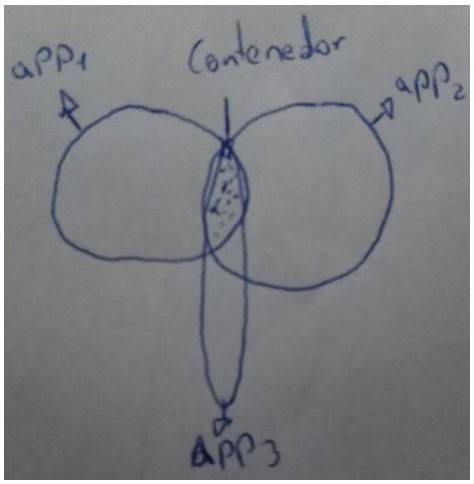
### Conecptos y anotaciones:

VPS: virtual private server.

LOPD, GPDR: normativas de protección de datos.

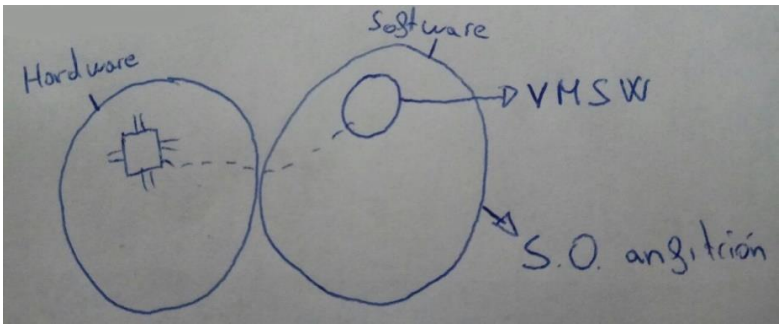
Serverless: modo de trabajo en el cual tú no tienes ningún servidor ni propio ni alquilado, sino que tú mandas un código a ejecutar (usando la API del servidor) y el servidor te devuelve el resultado. De esta forma no hay que preocuparse de mantenimiento ni inversión inicial.

Contenedor o Docker: un contenedor es una recopilación cerrada de aplicaciones, datos o recursos la cual permite ejecutar una determinada aplicación en cualquier SO permitiendo gran portabilidad.




Maquina virtual: una maquina virtual nos permite simular hardware (cogiéndolo de nuestra maquina) e instalar cualquier SO para hacer uso de el independientemente del SO anfitrión donde se esta ejecutando la máquina virtual.

VMSW: programa de virtualización (virtual box o VMware)



NEWS

# WUOLAH

LUN 29 OCT

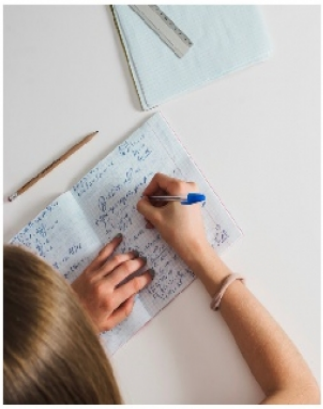
Noticias para el mundo universitario.

nº 1. Semana del 29 al 2

## CIEE oferta becas estudiantiles para los programas Intership USA y Work and Travel

*FCOM Videcanato de Movilidad y Relaciones Internacionales.*

CIEE, organización norteamericana sin ánimo de lucro que desarrolla y administra programas de estudios, voluntariado, prácticas y trabajos de verano en el extranjero; vuelve a ofertar becas para los programas Intership USA y Work and Travel. En la primera se posibilita realizar prácticas profesionales en una empresa o institución de EE.UU. relacionadas con la titulación del estudiante. Y bajo la modalidad más popular, Work and Travel, se ofrecen trabajos no cualificados en parques de atracciones, parques acuáticos, hoteles, restaurantes, etc. De EE.UU durante el verano.
Para más información puedes visitar: cieeseville.com



## Expulsados de la universidad varios alumnos por vender un examen

*Fuente: ultimahora.es*

La Universitat de Barcelona (UB) ha expulsado durante un periodo de dos años a cuatro estudiantes responsables del robo y la comercialización de un examen en julio de 2016, de la asignatura 'Fundamentos de la Fiscalidad' del tercer curso del grado de Administración y Dirección de Empresas (ADE), ha informado el centro en un comunicado este martes.

Ante la gravedad de los hechos, el centro puso el caso en manos de los Mossos d'Esquadra y, dos años después, la UB les ha sancionado con una expulsión temporal de la Facultad de Economía y Empresa, con la voluntad de actuar contra conductas fraudulentas en el ámbito académico que recoge el nuevo código ético.desconocido para el público general.
«Este tipo de conductas ponen de manifiesto, además de una falta absoluta de honradez académica, una actitud de desdén hacia las normas de convivencia y respeto» que deben regir las relaciones en la comunidad universitaria, ha afirmado la UB, que sentenció que no pueden ser toleradas.

## WUOLAH GIVEAWAY



### Fujifilm instax mini 9.

Fotografía todos tus viajes, tus fiestas, tus festivales...
Ahora no tendrás excusa para tener en fotos instantáneas todos tus recuerdos.

### Party&Co Extreme 3.0

Reune a todos tus amigos por que ya tenéis las risas aseguradas... Puedes ganar este Party&Co que seguro será el alma de la fiesta....

## Somos la primera cátedra de eSports en una universidad pública de todo el país.

*Fuente: www.diariosur.es*

Manuel Fernández Navas es el codirector de la Cátedra Estratégica de eSports de la Universidad de Málaga, que lidera el proyecto de investigación 'Brain Gamer'. Este estudio, que se encuentra en su segunda fase, tiene como objetivo observar el comportamiento psicofisiológico de los jugadores profesionales de videojuegos, los denominados eSports. Para ello colaboran el Ayuntamiento de Málaga, la Universidad de Málaga, la Universidad Internacional de La Rioja (UNIR) y la Sapienza de Roma, además de diferentes empresas como Vodafone Giant y la Liga Survival.

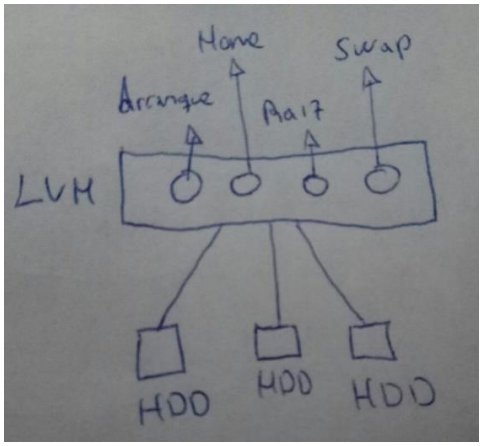
Algunos sistemas operativos:

- Solaris
- HP+
- LINUX
    - Ubuntu
    - CentOs

Vamos a utilizar las dos distribuciones de Linux para nuestras practicas

FDE: full disk encription

LVM: administrador de volúmenes lógicos de Linux. Nos permite crear volúmenes lógicos para ganar flexibilidad y poder redimensionar el espacio sin reiniciar siquiera.




RAID: redundant array of independent disks

es un sistema de datos con multiples unidades entre las cuales distribuye y replica los datos.

Un raid puede estar implementado en hardware o software.

| | Hardware | software |
|---|---|---|
| Expansibilidad | Menor | Mayor |
| Bug/virus | Menor | Mayor |
| Precio de despliegue | Mayor | Menor |
| eficiencia | mayor | Menor |

RAID0:

no duplica datos, solo reparte la información entre los diferentes discos para acelerar

la lectura/escritura

RAID1:

Crea copias exactas en los diferentes discos para aumentar la redundancia de datos y por tanto la seguridad

RAID5:

Divide los datos a nivel de bloque para obtener y almacenar la paridad para detectar y corregir errores. Tiene baja redundancia y necesita 3 discos como mínimo para poder implementarse.

RAID6:

Funciona igual que el 5 pero genera bloques de paridad duplicados y los distribuye entre todos los discos para una mayor seguridad.

## Realización:

### Instalación de Ubuntu

Características:

- 1GB RAM
- 5GB HDD .vdi x2 (tamaño fijo)
- Ubuntu 16.04

Usuario: jmab (iniciales del nombre)

Contraseña: pracitas,ISE

Usuario completo: jose maria aguilera barea

Nombre de la maquina: Ubuntu

No encriptar carpeta personal (porque vamos a hacer FDE)

Elegimos particionado manual

Creamos tabla de particiones en los dos discos

Creamos raid1

Configuramos LVM

Mantenemos distribución

Creamos grupo de volúmenes lógicos (lvm)

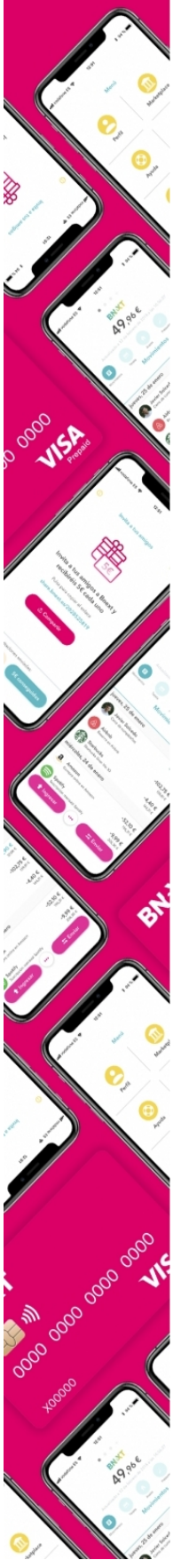
- Arranque 200MB
- Hogar 500MB
- Raíz restante
- Swap 1024MB

Después de esto ciframos todas las particiones menos el arranque

Y finalmente elegimos el sistema de archivos y el punto de montaje de cada volumen lógico

El MBR se instala en cualquiera de los dos discos, solo tener en cuenta que después tendremos que instalarlo en el otro disco con el siguiente comando:

Sudo grub-install /dev/sdb (en caso de haberlo instalado en el sda).



# Día 2

## Conecptos y anotaciones:

**diferencia entre cp /var , /var/.  Y cp/var/***

el primero, copia la carpeta en si dejandola en el destino como destino/var/contenidodevar.

el segundo, copia el contenido de var con todos sus archivos ocultos.

el tercero, copia el contenido de var con todos sus archivos (salvo los ocultos).

**SE linux**

Security-Enhanced Linux (SELinux) es un módulo de seguridad para el kernel Linux que proporciona el mecanismo para soportar políticas de seguridad para el control de acceso, incluyendo controles de acceso obligatorios como los del Departamento de Defensa de Estados Unidos.

**Atomicidad al copiar:**

las copias de seguridad de servicios en uso deben ser atómicas ya que un usuario puede escribir mientras se copia corrompiendo la información copiada. En Linux esto se soluciona cambiando el nivel de ejecución (monousuario) con el comando: *"systemctl isolate runlevel1.tarjet"*

**/etc/fstab**

Fichero donde se indican los puntos de montaje que se van a realizar siempre que encendamos el servidor.

## Algunos comandos:

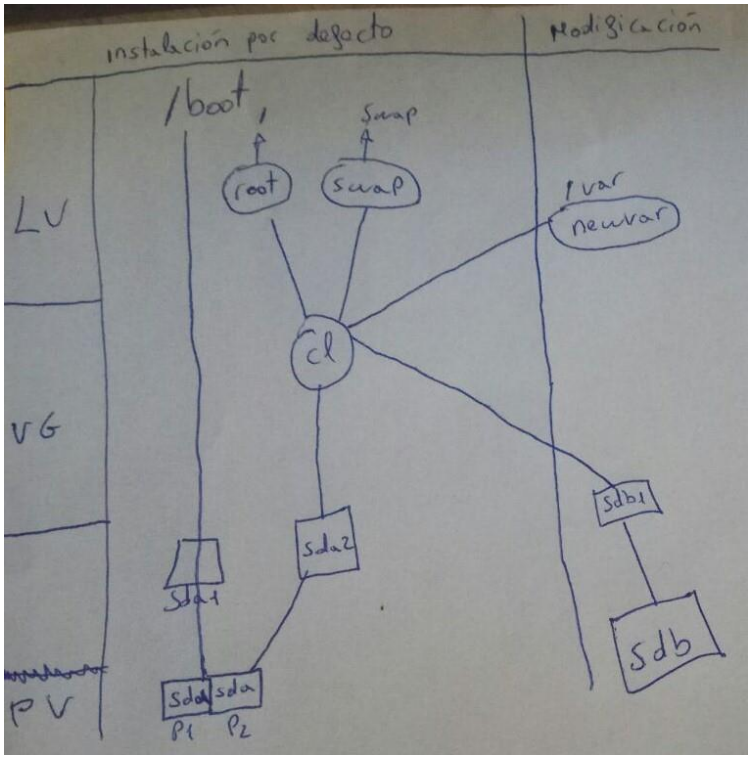
- **df -h**
  muestra el sistema de ficheros.
- **lsblk**
  Visualiza los dispositivos, unidades, particiones y sus capacidades (estén montadas o no).
- **Pvdisplay**
  Visualiza los volúmenes físicos.
- **Vgdisplay**
  Visualiza los grupos de volúmenes lógicos.
- **Lvdisplay**
  Visualiza los volúmenes lógicos.
- **Fdisk**
  Con esta herramienta podremos crear, eliminar, redimensionar, cambiar o copiar y mover particiones usando el sencillo menú que ofrece.

- **mount**
  sirve para montar particiones al sistema de archivos.
- **umount**
  sirve para desmontar particiones del sistema de archivos.
- **pvcreate**
  crea un volumen físico.
- **vgextend**
  crea un grupo de volúmenes lógicos.
- **Lvcreate**
  Crea un volumen logico
- **Mkfs**
  Crea una partición en un dispositivo o volumen lógico.
- **Restorecon**
  Restaura el contexto
- **vi**
  - **i**
    entra en modo inserción de texto.
  - **esc**
    entra en modo comando.
  - **:wq**
    Comando para guardar y cerrar el archivo.
  - **q!**
    comando para cerrar sin guardar.

## Realización:

### Instalación de centOs:

Creamos una maquina centOs por defecto en la instalación todo



## Como ampliar /var añadiendo un disco y separándolo de la raíz (para mas seguridad):

**Pasos:**

1. Añadir un nuevo disco a la maquina centOs
2. Crear sistema de archivos
    a. Crear volumen físico
    b. Extender el grupo de volúmenes
    c. Crear un nuevo volumen lógico
3. Hacer disponibles el volumen lógico (montar)
4. "copiar los datos de /var"
5. Asignar un nuevo punto de montaje
6. Liberar espacio

### 1. *Añadir nuevo disco en la maquina centOs*

En virtual box en el menú maquina→ configuración →almacenamiento → añadimos un disco sata nuevo

### 2. *Crear sistema de archivos*

Creamos el volumen fisico con: "Pvcreate /dev/sdb"

Para comprobar utilizamos "pvs"

Extendemos el grupo de volúmenes logicos cl con "ugextend cl /dev/sdb"

Comprobamos con "vgs"

Creamos un volumen lógico de 4G con nombre newvar en el grupo cl con "lvcreate -L 4G -n newvar cl"

### 3. *Copiar los datos de /var*

Creamos una partición en el volumen lógico con "mkfs -t ext4 /dev/cl/newvar

Creamos una carpeta fuera de la raíz para montar el volumen lógico con "mkdir /media/newvar"

Montamos el volumen lógico en la carpeta con "mount /dev/cl/newvar /media/newvar"

### 4. *Copiar los datos de /var*

Cambiamos el nivel de ejecución a monousuario con "systemctl isolate runlevel1.tarjet"

Copiamos los datos con "cp -ra /var/. /media/newvar" (la opción -ra copia recursivamente -r y copia todos los metadatos también -a)

### 5. *Asignar un nuevo punto de montaje*

Modificamos el fichero /etc/fstab con "vi /etc/fstab"

Añadimos la línea: /dev/mapper/cl-newvar /var ext4 defaults 0 0

Montamos los nuevos cambios con "mount -a"

### 6. *Liberar espacio*

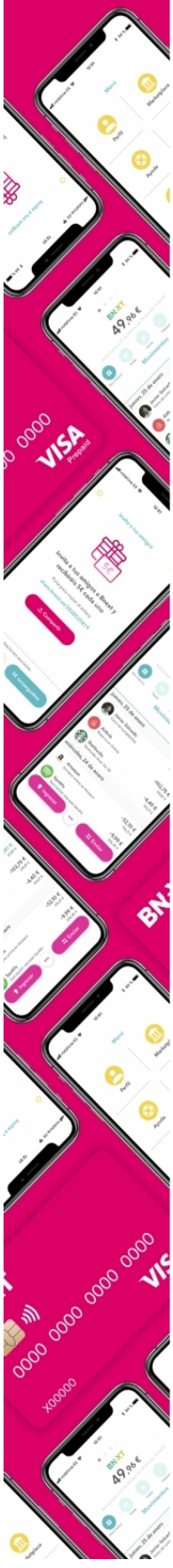
Desmontamos /dev/mapper/cl-newvar para que no haya varias carpetas apuntando al mismo bloque del disco con "umount /dev/mapper/cl-newvar

Movemos el contenido de var a una nueva carpeta de seguridad con “mv /var /varOLD

Creamos de nuevo la carpeta /var con “mkdir /var”

Restauramos el contexto de /var con “restorecon /var”

Montamos con la configuración actual con “mount -a”



# Dia 3

## Conceptos y anotaciones:

mdadm no está instalado por defecto en centOS para instalarlo: “yum install mdadm”

Da error porque no tenemos red.

En /etc/sysconfig/network-scripts/ifcfg-enp0s3 hay un atributo llamado onboot y está puesto a no.

Por esa razón da error la instalación. Levantando la interfaz de red ya debe funcionar.

En /etc/crypttab se guarda la configuración de los sistemas encriptados abiertos en el sistema

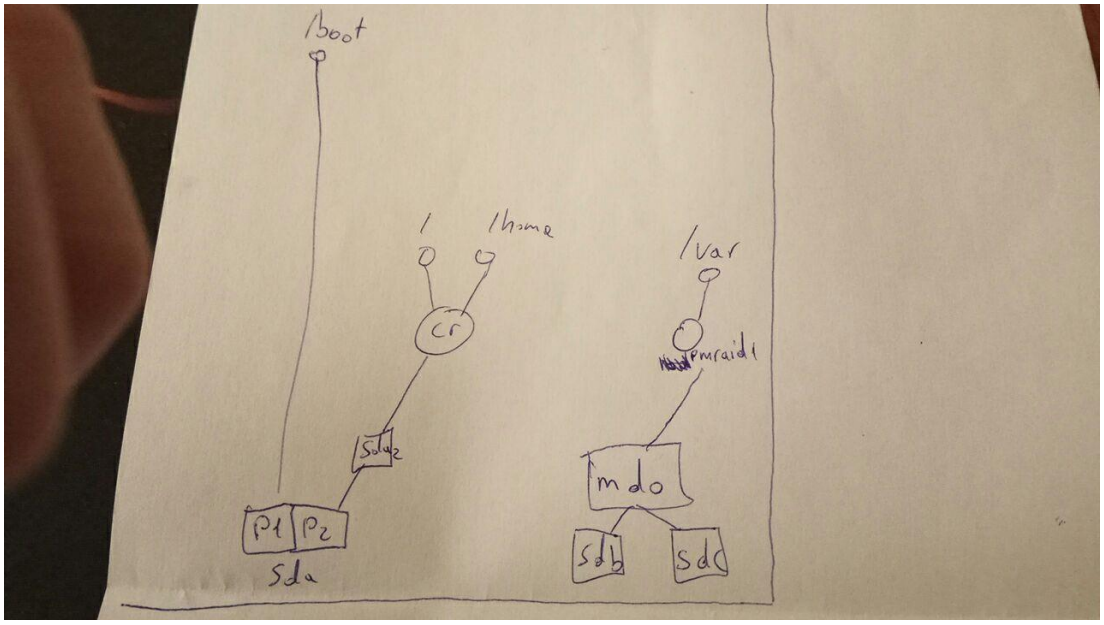
Usa el UUID

Para obtener el UUID de un disco con blkid nos lo muestra

## Algunos comandos:

- **mdadm** (multi device administrator)
  Sirve para administrar los raids en un sistema linux
- **ip add**
  Vemos las interfaces de red (como ifconfig, pero ifconfig esta obsoleto)
- **lspci**
  muestra el hardware en el bus pci (para maquinas virtuales es muy útil)
- **ipup <interfaz>**
  activa una interfaz de red
- **ifdown**
  desactiva una interfaz de red
- **shred**
  escribe basura en el disco para que nadie pueda modelar la función en caso de que tenga la información antes de cifrarla y después y pueda modelar la función de cifrado
- lsof
  muestra quien esta usando un recurso en especifico
- cryptsetup

## Realización:




Instalamos centOS por defecto

Vamos a configuración y añadimos 2 discos nuevos

Comprobamos que están los disco con el comando “lsblk”

Activamos la red con “ifup enp0s3”

Instalamos mdadm con “yum install mdadm”

Creamos el raid con “mdadm –create /dev/md0 –level=1 –raid-devices=2 /dev/sdb /dev/sdc”

Comprobamos con “lsblk”

Creamos un volumen físico con “pvcreate /dev/md0” (Se crea el volumen md0 para que el raid y el sistema estén separados)

Creamos un grupo de volúmenes lógicos con: “vgcreate pmraid1 /dev/md0”

Creamos un un volumen lógico en el grupo anterior con: lvcreate -L 1G -n newvar pmraid1

Entramos en modo monousuario: “systemctl isolate runlevel1.tarjet”

Le damos formato al volumen lógico con “mkfs -t ext4 /dev/mapper/pmraid1-newvar”

Creamos una carpeta para montar el volumen lógico y copiamos el contenido de var a esta con:

”mkdir /media/newvar”

“mount /dev/mapper/pmraid1-newvar /media/newvar/”

“cp -a /var/. /media/newvar/”

**Salimos del modo monousuario escribiendo “exit”**

Creamos copia de /var con “mv /var /varOLD”

Escribimos en el archivo de configuración /etc/fstab para que al inicio del sistema se monte el volumen lógico:

/dev/mapper/pmraid1-newvar  /var ext4 defaults 0 0

Hacemos efectivos los cambios, creamos el nuevo /var y restauramos el contexto con:

“mount -a”

“mkdir /var”

“restorecon /var”

“mount -a”

Comprobamos que todo está correcto con: “lsblk”

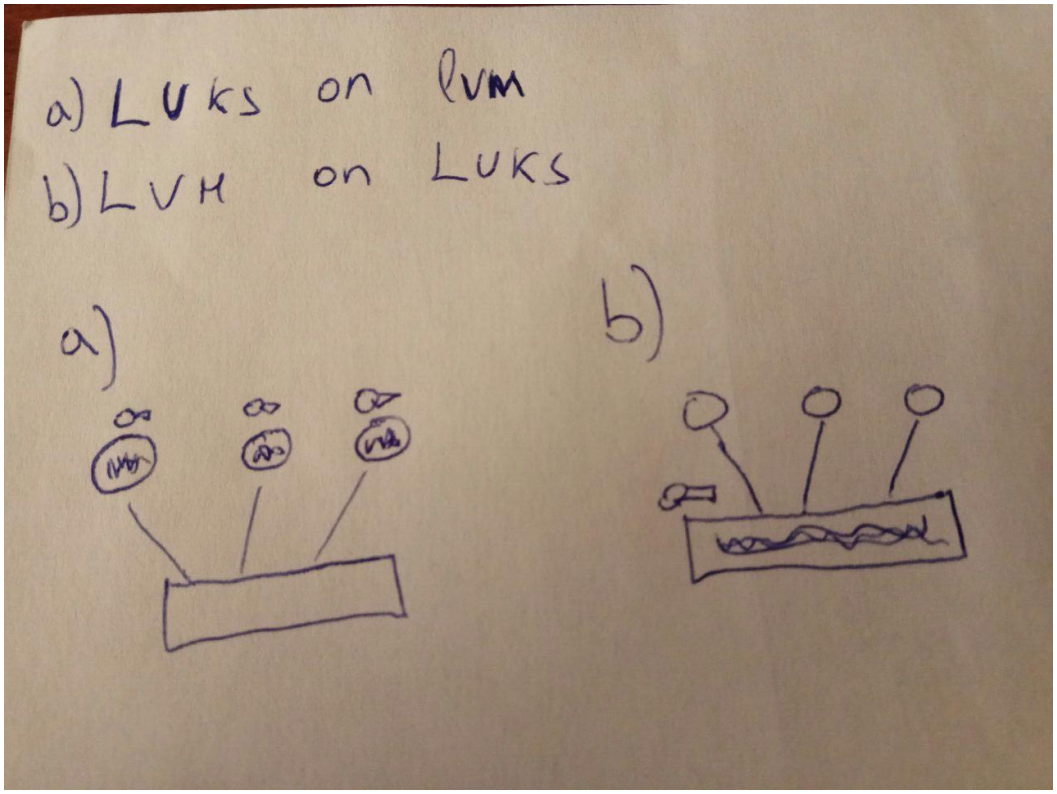
Desmontamos /media/newvar con: “umount /media/newvar/”

Ahora tenemos dos opciones encriptar cada volumen lógico o encriptar cada disco duro

a) luks on lvm

b) lvm on luks

usamos el **a** porque así cada volumen lógico podrá tener su clave independiente




para usar lucks debemos instalar cryptsetup

encendemos de nuevo la red con “ifup enp0s3” (se apago al entrar en el modo monousuario)

lo instalamos con “yum install cryptsetup”

copiamos el contenido de /var a la nueva carpeta /varRAID con “cp -a /var/. /varRAID”

intentamos encriptar el volumen logico con: “cryptsetupt lucksFormat /dev/mapper/pmraid1-newvar” (no nos deja porque pmraid1-newvar se está usando)

intentamos desmontar el volumen logico con: “umount /dev/mapper/pmraid1-newvar” (no nos deja porque pmraid1-newvar se está usando)

instalamos lsof con “yum install lsof”

ejecutamos “lsof /var” para saber quién está usándolo

matamos el proceso que lo está usando con: “kill -9 [numeroPID]”

desmontamos el volumen lógico “umount /dev/mapper/pmraid1-newvar”

encriptamos la información del volumen logico con: “cryptsetup lucksFormat /dev/mapper/pmraid1-newvar”

ya está cifrado, ahora para activarlo….

“cryptsetup luksOpen /dev/mapper/pmraid1-newvar pmraid1-newvar_crypt”

Para comprobar “ls /dev/mapper/” (debe aparecer ahi)

Creamos el sistema de ficheros con “mkfs -t ext4 /dev/mapper/pmraid1-newvar_crypt”

Creamos la carpeta donde se guardara la información encriptada con

“mkdir /media/newvar_crypt”

La montamos con “mount /dev/mapper/pmraid1-newvar_crypt /media/newvar_crypt”

Y copiamos la información de /varRaid a ella “cp -a /varRAID/. /media/newvar_crypt/”

**para montar el volumen cifrado automáticamente al inicio:**

Obtenemos el uuid del disco que necesitamos y lo metemos en el archivo /etc/crypttab con:

“blkid | grep crypto  >> /etc/crypttab”

Accedemos al fichero en cuestión con: “vi /etc/crypttab”

Y añadimos:

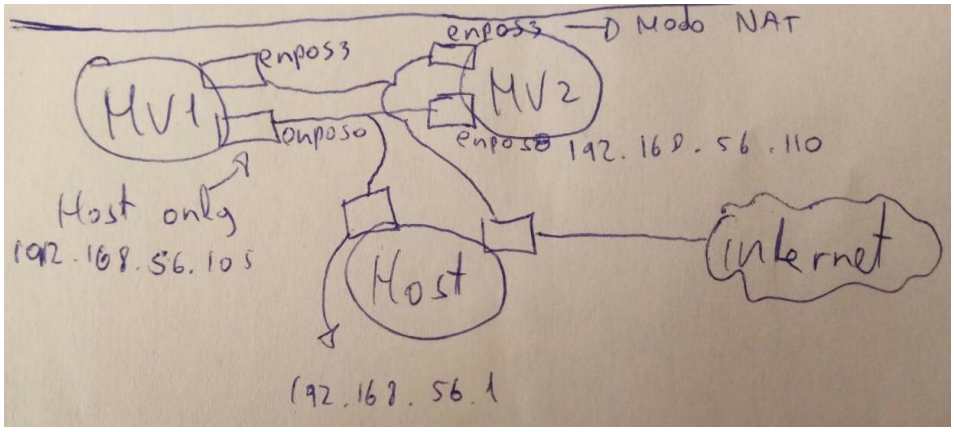
pmraid1-newvar_crypt UUID= …. None

accedemos al fichero /etc/fstab con “vi /etc/fstab”

y añadimos a la última línea que añadimos anteriormente en la ruta el _crypt

Reiniciamos y debe ir bien (pedirá la contraseña)

## Configuración de red de las maquinas virtuales




Para crear una red interna en virtual box debemos ir a archivo → preferencias → red

Aquí creamos una red con configuración 192.168.56.0/24

Después de esto, en cada maquina virtual debemos activar la segunda interfaz de red y seleccionarla en modo solo-anfitrión (host-only en inglés).

Esto se consigue en configuración→ red → adaptador 2.

PARA MODIFICAR LA CONFIGURACION DE RED EN LAS MAQINAS

Vi /etc/sysconfig/network-scripts/enp0s8

Borramos todas las líneas menos:

type

bootproto

name

device

onboot

Y añadimos

ipaddr=192.168.56.110 (caso de centOS)

ipaddr=192.168.56.110 (caso de Ubuntu)

además, si el atributo onboot está en OFF, ponerlo en ON

Tiramos la interfaz con: ifdown enp0s8

La levantamos con: ifup ifdown enp0s8