**Práctica 1: Lección 2**

***NO BORRAR LAS 3 PRIMERAS MÁQUINAS VIRTUALES***

1. Maquina nueva, CentOS8 Redhat 64bits 1024Mb, dico duro virtual ahora, vdi, reservado dinamicamente, 8GB tamaño de disco.

Conceptos: LV (volumen logico, swap, root,...), PV(volumen fisico, sda2), VG(grupo de volumenes

Vamos a tener dos particiones sda1 que tiene /boot y sda2 que tiene el grupo de volumenes, los volumenes logicos

Tenemos que incluir un nuevo disco sdb e incluirlo en VG y crear un nuevo volumen logico /var

Comandos

sudo fdisk /dev/sdb -> n -> p -> w

sudo pvdisplay -> 7GB -> 3 Gb para boot y 4Gb para pv

sudo vgextend cl /dev/sdb1

Ahora hay que montar el S.O para que pueda new\_var leer ficheros, ahora mismo es como si introducimos un pen drive y no lo ha montado el sistema.

0. Filesystem (mkfs -t ext4 /dev/cl/new\_var

1. Montar el LV

2. Copiamos

3. Revertir los cambios que hemos hecho

4. Liberación de memoria

ls -lZ / ->

cp funciona distinto en CentOS , se pierde el contexxto, por eso usamos cp -aç

ponemos sistema en modo manntenimiernto sudo systemctl rescue

entramos como root

systemctl rescue

systemctl status

cp -a /var/. /mnt/new\_var

cd/etc

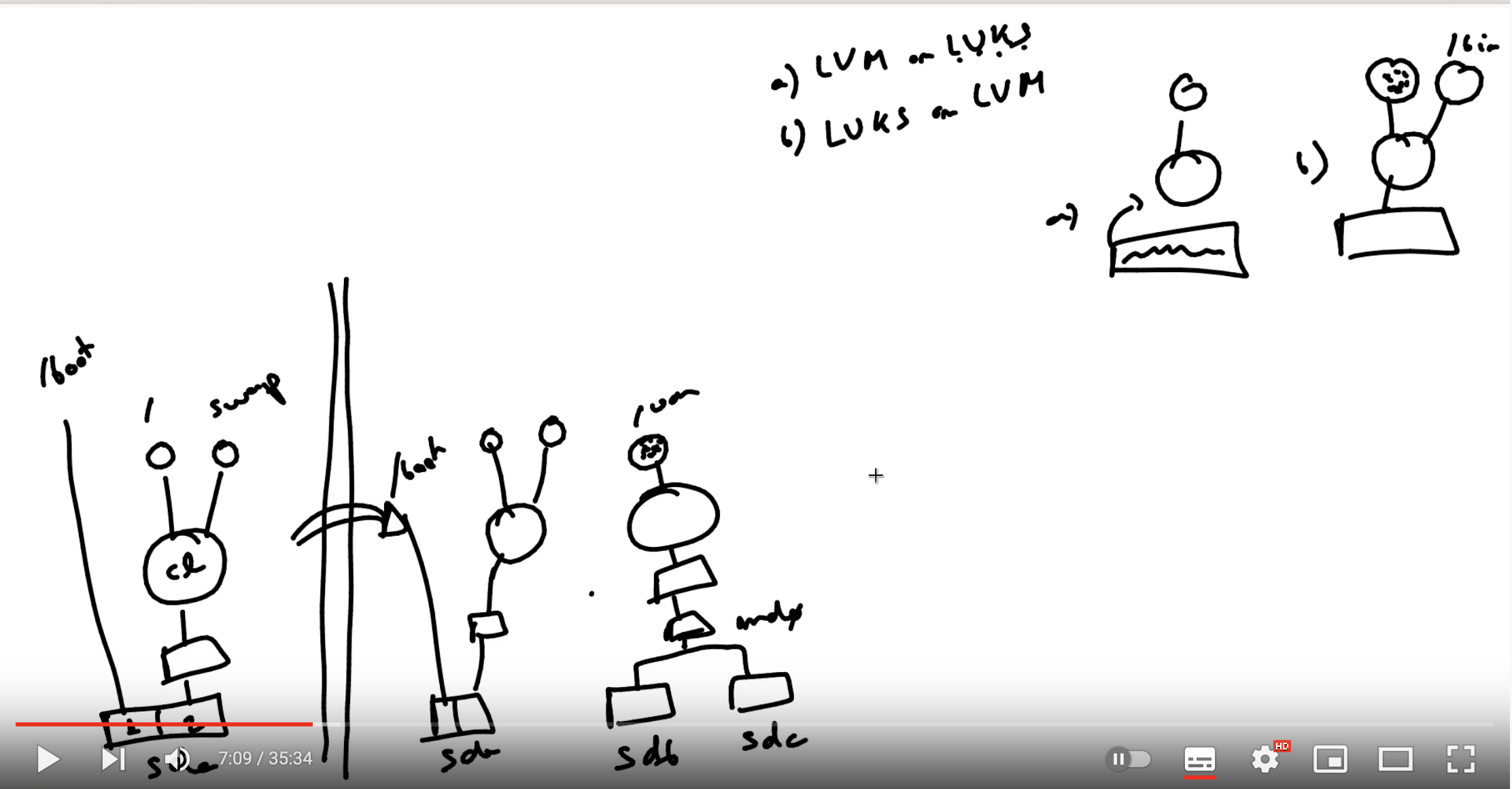
ahora tenemos que mapear

**Lección 3**

Configurar un RAID 1 y cifrar /var para que no se pierda la información.

Ubuntu: lvm on luks ---> más eficiente porque no tienes que introducir de nuevo la contraseña para encriptar parte del disco (cifrado del disco, una vez activado es formateado y se crea el VG y el LV)

CentOS: luks on lvm



En vez unir el nuevo LV /var a cl (VG) lo que hacemos es crear un nuevo VG al hacer el RAID 1, y creamos el nuevo módulo /var. No podemos unir el /var al volume group cl porque una vez que se crea el volume group no podemos cifrarlo por lo que debemos crear un nuevo volume group asociado al raid1 y encriptarlo.

COMANDOS Y PASOS

1. Crear maquina virtual CentOS.

2. Realizar RAID 1:

Creamos dos nuevos discos en la maquina virtual de 4GB

3. Iniciamos la maquina virtual

4. comprobamos con lsblk que estan bien montados

5. Necesitamos activar interfaz de red sudo ifup en0ps3 comprobamos con ping que fucniona

6. sudo fdisk /dev/sdb n p enter enter enter w

7. sudo mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sdb1 /dev/sdc1 (particion que era el raid de las otras dos particiones (md0 es una abstraccion logica de sdb1 sdc1

8. y

9. lsblk para comprobar

10. sudp pvs, sudo vgs

11. sudo pvcreate /dev/md0

12. sudo pvdisplay

enganchar volumen fisico a grupo de volumenes

13. sudo vgcreate clraid /dev/md0

14. sudo vgs

15. sudo lvcreate -n new\_var -L 1G clraid

16. sudo vgs

17. sudo lvdisplay

18. Para cifrar --> sudo cryptsetup luksFormat /dev/clraid/new\_var --> YES --> practicas,ise

sudo cryptsetup luksOpen /dev/clraid/new\_var clraid-new\_var\_crypt

sudo mkfs -t xfs /dev/mapper/clraid\_new\_var\_crypt (desencriptado)

Copiamos la infnormacion del antiguo /var al unevo

Creamos en mnt porque tiene carpeta auxiliar para volumenes logicos

mount /dev/mapper/clraid-new\_var\_crypt /mnt/new\_var

systemctl isolate rescue entramos como root y hacemos de nuevo systemctl isolate rescue para entrar en status mainteinance

cp -a /var/. /mnt/new\_var

ls -lZ /mnt/new\_var

sudo mv /var /var\_old

mkdir /var

restorecon /var

vi /etc/fstab modificamos y añadimos /dev/mapper/clraid-new\_var\_crypt /var xfs defaults 0 0

blkid y queremos la encriptada

blkid | grep crypto

blkid | grep crypto > /etc/crypttab abrimos con vi /etc/crypttab borramos comillas de uuid /etc/crypttab lo de type y ponemos none y añadimos al clraid-new\_var\_crypt

umount /mnt/new\_var

mount -a