Sesión 1.

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), cirtual machine software

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.

	HW	SF
Expansibilidad	Menor	Mayor
Bug/Virus	Menor	Mayor
Precio	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.

MBR: Mates Boot Record, registro de arranque principal, conocido también.

Instalación de ubuntu: /* muchas veces hecha */

Sesión 2.

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.

df -h: Muestra el sistema de ficheros.

lsblk: Visualiza los dispositivos, unidades, particiones y sus capacidades (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:

- Con i entra en modo inserción de texto.
- Con esc entra en modo comando.
- Con :wq Comando para guardar y cerrar el archivo. o q! comando para cerrar sin guardar.

Instalación de CentOS: /* Todo por defecto */

Aplicar /var añadiendo un nuevo disco:

1. Añadir un nuevo disco a la maquina CentOs
2. Crear sistema de archivos.
    1. Crear volumen físico
    2. Extender el grupo de volúmenes
    3. 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 un nuevo disco a 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”

Sesión 3.

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)

blkid: Obtener tipo de partición, UUID y el identificador del nodo

ipup <inferfaz>: muestra el hardware en el bus pci (para maquinas virtuales es muy útil) • ipup

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: Herramienta que usamos para emcriptar el disco duro.

Crear RAID1 en CentOs para /var:

- 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 activamos “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”

- 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 necesitamoslo 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 Red en UBUNTU:

Configuración Red CentOs: