PART TEÒRICA UF4: Seguretat, Rendiment i Recursos

**Logical Volume Manager (LVM):**

Permet crear grups de volums a partir de volums físics i dividir aquest en volums lògics.

D’aquesta manera podríem dir que primer reconeix els discos durs o les particions que volem agafar com a volums físics, a partir d’un o més d’aquest crea un grup de volums (ho podríem comparar amb un disc virtual) i per finalitzar es creen els volums lògics que serien una mena de particions dels grups de volums.

**Zettabyte File System (ZFS):**

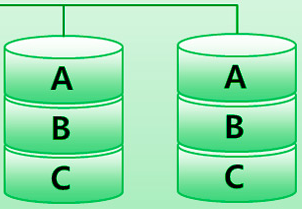
És un sistema d'arxius de codi obert de característiques avançades. Compta amb un gran nombre de mesures de protecció de dades amb sistemes d'integritat contra la pèrdua i corrupció

**RSYNC:**

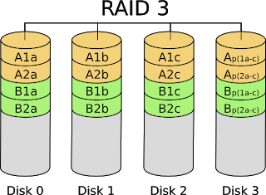
És una eina per a sincronitzar els fitxers i directoris que tenim emmagatzemats en un lloc en un altre diferent minimitzant la transferència de dades

**Tipus de RAID:**

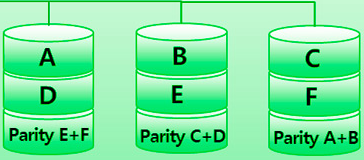
RAID 1: Funciona afegint discos rígids paral·lels als discos rígids principals existents en la computadora



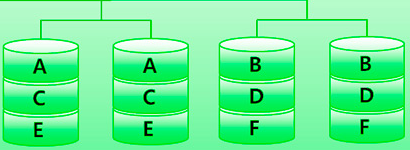
RAID 3: Les dades són dividides entre els discos de la matriu, excepte un, que emmagatzema informació de paritat



RAID 5: Aquest nivell de RAID és molt semblant al Nivell 4, excepte pel fet que la paritat no està destinada a un únic disc, sinó a tota la matriu



RAID 0+1: És una combinació dels nivells 0 (Striping) i 1 (Mirroring), on les dades són dividides entre els discos per a millorar l'ingrés, però també utilitzen altres discos per a duplicar la informació.



**Criptografia:**

Aspectes a tenir en compte en la criptografia:

* Confidencialitat
* Integritat: Les dades no han estat canviades
* Autentificació: El receptor pot verificar qui ha enviat el missatge
* No Repudi: El que envia el missatge no pot denegar que ho ha fet

Tipus de Xifrat:

* Xifrat Simètric:

Només utilitza una clau. Si volem enviar-li un correu a un altre usuari, xifrem aquest missatge amb una clau.

* Xifrat Asimètric:

Utilitza dues claus en aquest cas. Una privada i una altra pública. La clau pública serveix per a xifrar aquest correu i la privada per a desxifrar-lo.

* Mètodes Hibrids:

Farem combinacions dels dos tipus de xifrats

**Tipus de Bckups:**

– Còpia de seguretat completa:

Fa una copia completa de tots arxius del nostre equip.

– Còpia de seguretat diferencial:

Únicament conté els arxius que han canviat des de l'última vegada que es va fer la còpia total. Per tant s'inclouen només els arxius nous i/o modificats.

– Còpia de seguretat incremental:

És fa una còpia de tots els arxius que han estat modificats des que va ser executat l'última còpia de seguretat completa, diferencial o incremental.

**Monitoratge:**

Eines de monitoratge a Windows:

Monitor de recursos

* Permet la supervisió en temps real de diferents components del sistema i també informació sobre com els processos i serveis utilitzen aquests recursos

Monitor de rendiment

* El monitor de rendiment de Windows és una eina complexa i molt completa que proporciona diverses utilitats per analitzar el rendiment del sistema

Eines de monitoratge de rendiment a Linux:

* **uptime**. Dóna l’hora del sistema, el temps que fa que està encès, la quantitat d’usuaris connectats i la càrrega mitjana del sistema durant l’últim minut, els últims cinc minuts i els últims quinze minuts.
* **time**. Permet executar una ordre o aplicació i enregistrar els recursos que ha emprat
* **vmstat**. Dóna informació de l’estat de la memòria física, de la memòria virtual, de la de intercanvi
* **free**. Utilització de la memòria del sistema. Concretament, la memòria total, la memòria en ús, la memòria lliure
* **df**. Utilització de disc. Per a cada unitat muntada, mostra l’espai utilitzat i l’espai lliure.
* **du**. Utilització de disc. Per a cada directori mostra l’espai utilitzat
* **hdparm**. Mostra el valor dels paràmetres més importants d’un disc i permet modificar-ne alguns
* **netstat**. Informació de l’estat de la xarxa del sistema. Dóna protocols, quantitats de bytes d’entrada i sortida, origen i destinació de la comunicació

Eines de gestió de tasques i processos en Linux:

* **ps**. permet visualitzar els processos en execució
* **pstree**. Aquesta ordre mostra una llista de processos en forma d’arbre seguint la jerarquia de processos
* **top**. Correspon a la presentació interactiva dels processos, en temps real
* **kill, killall**. Aquestes dues ordres es fan servir per enviar senyals a processos
* **nice, renice**. El primer permet arrencar un procés assignant-li una prioritat determinada, mentre que **renice** permet canviar la prioritat d’un procés ja endegat

Auditoria:

Per modificar les directives de seguretat local, tenim que anar a Directivas de Seguridad Local, allà dins trobarem tot el necessari

PART PRÀCTICA UF4: Seguretat, Rendiment i Recursos

**LVM:**

Per tal de crear-los les tres comandes principals són:

pvcreate <disc1> <disc2> etc. Per reconeixer els volums físics.

vgcreate -v nomvgrup <disc1> <disc2> etc. Per tal d’afegir els discos físics a un grup de volums.

lvcreate -n label -L mida <nomvgrup>. Per crear una partició d’aquest grup de volums.

mkfs.ext4 /dev/VolumeGroup/Logical0: Formatar el volum lògic

vgdisplay: Veure informació sobre el LVM

pvs: Veure volums físics

sudo vgextend [nom del grup de volums] [lloc on volem estendre el VG]: Estendre el grup de volums

lvextend –L +2GB [lloc que redimensionar]: Estendre el volum lògic

**Comandes RAIDs:**

Mdadm –create –verbose /dev/mdX –level=1 –raid-devices=2 /dev/mdX1 /dev/mdX2: Serveix per crear el RAID

Mdadm –query –detail /dev/mdX: Per veure en detall un dels elements del raid

Cat /proc/mdstat: Comprovar l’estat del RAID

Mdadm –stop /dev/mdX: Per aturar un array

Mdadm –assemble /dev/mdX: Per engegar l’array

Mkfs.ext4 /dev/mdX: Donar format al RAID

**Creació ZFS:**

Apt-get install zfsutils-linux

Creació del pool : Zpool create –f –m /data pool1 /dev/sdb /dev/sdc

Crearem un subvolum : Zfs create pool1/sub2

Veure el zpool : Zfs list: Veure el zpool

Exportar el zpool : Zpool export pool1

Importar el zpool : Zpool import pool1

**Encriptació LUKS:**

Instal·lar cryptsetup : Apt-get install cryptsetup

Shred –verbose –random-sources=/dev/urandom –iterations=1 /dev/sdb1

Comanda per encriptar el disc :

Cryptsetup –verbose –cipher aes-xts-plain64 –key-size 512 –hash sha512 –iter-time 5000 –use-random luksFormat /dev/sdb1

Cryptsetup open –type luks /dev/sdb1 root

**RSync:**

Fer una copia incremental nomes dels fitxers que hagin canviat i esborri de tmp tots els fitxers que no estiguin al /home :

Rsync –a –delete /home/xavi/\*\* /tmp

**Crontab:**

**Nano /etc/crontab**

**Format del fitxer Crontab**  
  
\* \* \* \* \* Commanda a executar  
- - - - -  
| | | | |  
| | | | +----- Dia de la setmana (0-6)  
| | | +------- Mes (1 - 12)  
| | +--------- Dia del mes (1 - 31)  
| +----------- Hora (0 - 23)  
+------------- Minut (0 - 59)

**Recuperació del Sistema - GRUB:**

Modifiquem el fitxer grub perquè no arrenqui

Arrenquem amb un livecd de ubutu

Mkdir mylinux

Muntar la partició del disc dur : Mount /dev/sda1 /mnt/mylinux

Muntar les carpetes especials : Mount –t proc proc /mnt/mylinux/proc

Muntar les carpetes especials : Mount –t sysfs sys /mnt/mylinux/sys

Muntar les carpetes especials : Mount –o bind /dev /mnt/mylinux/dev

Canviar el sistema arrel amb chroot : Chroot /mnt/mylinux/ /bin/bash amb chroot

Actualitzar el grub : Update-grub

Actualitzar el grub : Grub-install /dev/sda

**Directives de Seguretat Local:**

Per canviar qualsevol configuració anirem a directiva de Seguridad local, Directivas Locales – Opciones de Seguridad i en Directivas de cuenta -- contraseñas