Fase 4 - Activitat 10: Gestió bàsica de tasques automatizades amb systemd

1- Identificació del grup i activitat:

Curs: ASIX2
Projecte: PJ6 Administració de xarxes i sistemes operatius
Fase: 4
Activitat: 10
Grup/Individual: Individual

2- Objectius de l'activitat

a) Utilització de **rsync** sobre **ssh** per dur a terme la tasca de creació còpies de seguretat.
b) Utilització de **systemd** per planificar i automatizar la tasca de creació de còpies de seguretat.

3- Conceptes

a) L'eina **rsync**:

- És una eina per sincronitzar arxius locals i remots. És a dir, permet copiar arxiu locals en equips remots mantenint no només el nom i les dades sino també altres informació important com per exemple l'usuari propietari, permisos, data de creació,....
- És una eina eficient perquè permet minimitzar la quantitat de dades enviades. Si un arxiu ja existeix però ha estat modificat, s'enviaran únicament les parts de l'arxiu que han canviat.
- És una eina que està disponible per qualsevol distribució de GNU/Linux o Unix.
- És una eina útil per crear scripts que permeten fer backups de sistema.

b) Què és **systemd** i que són els **temporitzadors** de **systemd**?

- **systemd** és l'eina de gestió global del sistema i també de control del seu procés d'arrancada.
- És l'eina utilitzada per la majoria de distribució de GNU/Linux actualment.
- Els **temporitazadors** de **systemd** (o **systemd timers** en anglès) permeten automatitzar l'inici d'un procés, programa, script o ordre a una hora determinada o en intervals de temps determinats.
- Aquí trobareu més informació sobre els **temporitzadors** de **systemd**.

c) Combinant **rsync** sobre **ssh**, **scripts** del bash i **systemd** poden crear un sistema de realització de **còpies de seguretat** (backups) de la complexitat que vulguem. Aquesta és una tasca típica d'administració de sistemes operatius en xarxa.

4- Insta·lació i muntatge d'un disc dur per les còpies de seguretat en el servidor

a) Afegeix a **srv-pj6** un nou disc de **100 GiB**. Amb **GParted** (que pots instal·lar en el servidor) fes que el nou disc tingui una taula de particions **GPT** i només una partició de tipus **Ext4** amb l'etiqueta **CòpiesSeguretat** que utilitzi tot el disc.

b) Crea un punt de muntatge (és a dir, un directori) dins de **/mnt** i de nom **copSeg.**

c) Identifica la **UUID** de la partició del disc dur de **100GiB** i fes que durant l'arrancada del sistema es munti automàticament la partició dins del directori **/mnt/copSeg**.

d) Si es munta automàticament, fes que:

- El **propietari** (recursivament) del directori sigui el teu usuari normal.
- El **group** (recursivament) del directori sigui **backup** (un grup que ja existeix)
- Els permisos pel **propietari** siguin de **lectura/escriptura/execució** sobre el directori.
- Els permisos del grup **backup** siguin de **lectura/execució** sobre el directori.
- Els grup **others** no tingui cap permís d'accés al directori.

e) Comprova, abans de continuar, que el sistema arranca, que es munta el disc, i que els permisos i propietaris són correctes.

f) Finalment crea un directori de nom **xxyyzz-cli-pj6** (que és el nom de sistema del client) dins de **copSeg** amb els mateixos permisos i propietaris que **copSeg**.

5- Creació d'un script del bash utilitzant rsync sobre ssh per fer còpies de seguretat del directori /home del client en el servidor.

a) Dins del **servidor** i el **client** instal·la **rsync**.

b) Comprova que pots fer una connexió **ssh** directa com vas fer a l'activitat 6 des del client al servidor. Ho hauries de poder si tenies avaluada aquella activitat.

c) Crea un script del bash dins del **client** amb el nom **copSeg.sh** i amb el següent contingut:

```
#!/bin/bash
DATA=$(date +20%y%m%d%H%M%S)
ORIGEN=/home/
DESTINACIO=/mnt/copSeg/xxyyzz-cli-pj6/home_$DATA
USUARI=xxyyzz
SERVIDOR=xxyyzz-srv-pj6.clotfje.net

rsync -avzh --delete --stats $ORIGEN  $USUARI@$SERVIDOR:$DESTINACIO
exit 0
```

A on xxyyzz s'han de canviar per l'identificador d'usuari i equip del teu servidor.

d) Desa el script dins del director **/usr/sbin** amb els permisos **rwx** per **root**, **r-x** pel **grup root** i cap permís per la resta d'usuaris.

e) Fes que l'usuari **asix2** del client tingui permisos **r-x** sobre el script **copSeg.sh** utilitzant ACL com vam veure dins de l'activitat de SAMBA a l'apartat **4.4** punt **d)**.

e) Comprova que el script funciona. S'hauria de crear una copia de seguretat del directori **/home** del client dins del servidor amb la data inclosa.

NOTA: En funció de la grandària del directori **/home**, la velocitat de la xarxa i dels equips, la còpia pot trigar des d'uns segons a uns minuts.

6- Creació d'un servei de Systemd per iniciar el script

a) Dins del directori **/etc/systemd/sytem** del client crea un arxiu de nom **copSeg.service**.

b) Fes que tingui el següent contingut:

```
[Unit]
Description= Servei de copies de seguretat
Requires=network.target
After=network.target

[Service]
Type=simple
ExecStart=/usr/sbin/copSeg.sh
User=asix2
```

c) Executa la següent ordre per fer que el sistema detecti el nou servei: **sudo systemctl daemon-reload**

d) Comprova que el servei funciona:

- Executa: **sudo systemctl start copSeg.service**
- Comprova que es crea una nova còpia de seguretat dins del servidor.
  NOTA: En funció de la grandària del directori **/home**, la velocitat de la xarxa i dels equips, la còpia pot trigar des d'uns segons a uns minuts.

7- Creació d'un temporitzador de Systemd per planificar i automatizar les còpies de seguretat

a) Dins del directori **/etc/systemd/sytem** del client crea un arxiu de nom **copSeg.timer**.

b) Fes que tingui el següent contingut:

```
[Unit]
Description= Temporitzador del servei de copies de seguretat

[Timer]
Unit=copSeg.service
OnCalendar=*-*-* 14:00:00

[Install]
WantedBy=timers.target
```

NOTA 1: Aquí trobareu una taula amb el funcionamen del paràmetre **OnCalendar**.

c) Canvia l'hora del paràmetre **OnCalendar** per poder fer una prova de funcionament a classe.

c) Executa la següent ordre per fer que el sistema reconegui el timer: **sudo systemctl daemon-reload**

d) Habilita i inicia el timer. Executa:
- **sudo systemctl enable copSeg.timer**
- **sudo systemctl start copSeg.timer**

e) Comprova el seu estat: **sudo systemctl status copSeg.timer**. Ha de sortir el dia i hora a la qual has fixat el temporitzador.

f) Comprova que s'ha afegit el timer a la llista de timers: **sudo systemctl list-timers -all**

g) Comprova que es crea una nova còpia de seguretat dins del servidor automàticament a l'hora indicada.

NOTA 2: En funció de la grandària del directori **/home**, la velocitat de la xarxa i dels equips, la còpia pot trigar des d'uns segons a uns minuts.

h) Si voleu canviar l'hora de la còpia de seguretat hareu de:
- Modificar copSeg.timer
- Executar **sudo systemctl daemon-reload**

Lliurament de la pràctica

1- Data d'inici de lliurament:
- 11-12-2025 de 19.10 a 21.00

2- Comprovacions:
- Es demanarà la modificació de l'hora de creació de la còpia de seguretat i es comprovarà que es realitza a l'hora demanada.
- Es comprovarà que la còpia de seguretat es desa en el segon disc dur del servidor.