⚒️ AF.3.1.12 — Administració d'SSH amb Webmin a través d'un túnel SSH

En esta activitat instal·lem **Webmin** en una instància Ubuntu Server d'AWS Academy i hi accedim des del navegador del client **Linux Mint** sense obrir cap port nou al grup de seguretat: tot el trànsit viatja dins d'un **túnel SSH local** (`ssh -L`). Després fem servir Webmin per revisar les opcions de seguretat del servidor SSH i la política d'accés per usuaris i grups.

Abans de començar, convé haver llegit Túnels i redirecció de ports i El servidor SSH.

Escenari

```
flowchart LR
    subgraph CLI["🏫 Aula"]
        MINT(["🐧 <b>Linux Mint</b><br/>🌐
navegador<br/>https://localhost:10000"])
    end

    subgraph AWS["☁️ AWS — grup de seguretat: només 🔓 22 · 🚫 10000"]
        SSHD{{"🔐 <b>sshd</b> :22"}}
        WEBMIN["🌐 <b>Webmin</b><br/>localhost:10000"]
    end

    MINT == "🔐 ssh -L 10000:localhost:10000<br/>(trànsit xifrat)" ==> SSHD
    SSHD -- "localhost:10000" --> WEBMIN

    classDef mint fill:#2e9e5b26,stroke:#2e9e5b,stroke-width:2px
    classDef sshd fill:#12919a40,stroke:#0b6e75,stroke-width:3px
    classDef web fill:#e9542026,stroke:#e95420,stroke-width:2px
    class MINT mint
    class SSHD sshd
    class WEBMIN web

    style CLI fill:#d977060d,stroke:#d97706,stroke-width:2px,stroke-
dasharray:6 4
    style AWS fill:#ff99000d,stroke:#ff9900,stroke-width:2px,stroke-
dasharray:6 4

    linkStyle 0 stroke:#0b6e75,stroke-width:3px
    linkStyle 1 stroke:#e95420,stroke-width:2px
```

Element	Valor a l'exemple
Servidor	Instància EC2 amb Ubuntu Server, usuari `ubuntu`
Client	Linux Mint amb navegador web
Clau privada	`labsuser.pem` descarregada d'AWS Academy
Grup de seguretat	Només SSH (22/TCP): grup `ssh-extern` (píndola UDXX-02-2 d'AWS Academy)
`<IP_PUBLICA>`	IP pública de la instància (canvia en cada inici del lab)

> **Informació**
>
> Si encara no teniu la instància, seguiu la píndola **UDXX-03 — Desplegament d'una màquina virtual Ubuntu Server a AWS Academy** de l'apartat AWS Academy.

1. Connectar a la instància i instal·lar Webmin

Des del terminal de Linux Mint, connectem amb la clau privada (els permisos han de ser restrictius o `ssh` la rebutjarà):

```
chmod 400 ~/Baixades/labsuser.pem
ssh -i ~/Baixades/labsuser.pem ubuntu@<IP_PUBLICA>
```

Ja dins de la instància, instal·lem Webmin des del seu repositori oficial:

```
curl -o webmin-setup-repo.sh
https://raw.githubusercontent.com/webmin/webmin/master/webmin-setup-repo.sh
sudo sh webmin-setup-repo.sh
sudo apt-get install webmin --install-recommends
```

Comprovem que el servei està actiu i que escolta al port 10000:

```
systemctl status webmin
sudo ss -tlnp | grep 10000
```

> ⚠ **Atenció**
>
> **No obrim el port 10000 al grup de seguretat.** Webmin dona control total del servidor; publicar-lo a Internet l'exposaria a atacs de força bruta. L'accedirem només a través del túnel SSH.

2. Crear el túnel SSH des de Linux Mint

Obrim **un altre terminal** al client i creem una redirecció local: el port 10000 del Linux Mint es connecta, a través de SSH, amb el port 10000 de la pròpia instància (`localhost` vist des del servidor).

```
ssh -i ~/Baixades/labsuser.pem -N -L 10000:localhost:10000 ubuntu@<IP_PUBLICA>
```

Part	Significat
`-L 10000:localhost:10000`	Port local 10000 → `localhost:10000` vist des de la instància
`-N`	No obri cap shell: només manté el túnel
`-i labsuser.pem`	Clau privada per autenticar-nos

El terminal queda "parat": és normal, el túnel està obert mentre la connexió continue activa. Per tancar-lo, `Ctrl`+`C`.

Ara, al navegador del Linux Mint obrim:

```
https://localhost:10000
```

El navegador avisarà que el certificat no és de confiança: Webmin usa un **certificat autosignat**. Acceptem el risc per continuar (el trànsit, a més, ja viatja xifrat dins del túnel SSH).

> ⓘ **Informació**
>
> Si el port 10000 ja està ocupat al client, podem usar-ne un altre local: `-L 8443:localhost:10000` i obrir `https://localhost:8443`.

3. Usuari per entrar a Webmin

Webmin autentica amb els **usuaris del sistema**: permet entrar com a `root` o amb qualsevol usuari que puga executar ordres com a root amb `sudo`. A AWS, l'usuari `ubuntu` té `sudo`, però **no té contrasenya** (entrem per SSH amb clau). Per això li n'assignem una des de la sessió SSH:

```
sudo passwd ubuntu
```

Ara ja podem iniciar sessió a Webmin amb l'usuari `ubuntu` i la contrasenya que acabem de definir.

> ⚠ **Atenció**
>
> Esta contrasenya és per a **Webmin** (i per a `sudo`). **No activa** l'accés SSH amb contrasenya: el servidor SSH continua acceptant només claus, tal com veurem al pas següent. Feu servir una contrasenya robusta.

4. Revisar la seguretat del servidor SSH amb Webmin

A Webmin anem a **Servers → SSH Server** (*Servidors → Servidor SSH*). El mòdul edita `/etc/ssh/sshd_config` i agrupa les opcions en apartats. Revisem l'apartat **Authentication**:

Opció a Webmin	Directiva `sshd_config`	Valor recomanat a AWS
Allow authentication by password?	`PasswordAuthentication`	`no`
Permit logins with empty passwords?	`PermitEmptyPasswords`	`no`
Allow login by root?	`PermitRootLogin`	`no`
Allow RSA authentication?	`PubkeyAuthentication`	`yes`

Contrasenya o clau?

Mètode	Avantatges	Inconvenients
Només contrasenya	Senzill: no cal distribuir claus	Vulnerable a força bruta i a contrasenyes febles o reutilitzades
Només clau pública	Molt resistent a força bruta; sense secret per la xarxa	Cal custodiar la clau privada; si es perd, es perd l'accés

En un servidor exposat a Internet, com una instància d'AWS, la pràctica recomanada és **deixar només l'autenticació amb clau** (`PasswordAuthentication no`), que és el que porten per defecte les imatges d'Ubuntu d'AWS.

Perill

On està realment la configuració? A Ubuntu, `sshd_config` comença amb `Include /etc/ssh/sshd_config.d/*.conf`, i OpenSSH es queda amb el **primer valor** que llig de cada directiva. Les imatges d'AWS porten `/etc/ssh/sshd_config.d/60-cloudimg-settings.conf` amb `PasswordAuthentication no`, de manera que **canviar esta opció des de Webmin no té cap efecte** mentre existisca eixe fitxer.

Comproveu sempre la configuració **efectiva** amb:

```
sudo sshd -T | grep -Ei
'passwordauthentication|pubkeyauthentication|permitrootlogin'
grep -r . /etc/ssh/sshd_config.d/
```

5. Política d'accés per usuaris i grups

A l'apartat **Access Control** del mòdul SSH Server trobem quatre camps:

Opció a Webmin	Directiva	Efecte
Only allow users	`AllowUsers`	Només poden entrar els usuaris de la llista

Opció a Webmin	Directiva	Efecte
Only allow members of groups	`AllowGroups`	Només poden entrar els membres (grup primari o secundari)
Deny users	`DenyUsers`	Els usuaris de la llista no poden entrar
Deny members of groups	`DenyGroups`	Els membres dels grups de la llista no poden entrar

OpenSSH les comprova en este ordre: `DenyUsers`, `AllowUsers`, `DenyGroups` i `AllowGroups`. Un usuari ha de **superar totes** les que estiguen definides; per tant, si s'omplen alhora `AllowUsers` i `AllowGroups`, l'usuari ha de complir **les dues** condicions. Per evitar sorpreses, és millor triar **una sola estratègia**: normalment, un grup d'accés (`AllowGroups`).

Exemple: només el grup `sshusers` pot entrar per SSH

Preparem, des de la sessió SSH, un grup d'accés i un usuari de prova que **no** hi pertany. Li copiem la clau autoritzada d'`ubuntu` perquè puga entrar amb la mateixa clau:

```
sudo groupadd sshusers
sudo usermod -aG sshusers ubuntu

sudo adduser --disabled-password --gecos "" prova
sudo install -d -m 700 -o prova -g prova /home/prova/.ssh
sudo install -m 600 -o prova -g prova ~/.ssh/authorized_keys /home/prova/.ssh/
```

Abans de restringir res, comprovem des de Linux Mint que `prova` pot entrar:

```
ssh -i ~/Baixades/labsuser.pem prova@<IP_PUBLICA> hostname
```

Ara, a Webmin → **SSH Server** → **Access Control**, a **Only allow members of groups** escrivim `sshusers`, desem i polsem **Apply Changes** perquè es reinicie el servei. Comprovem la configuració efectiva i tornem a provar:

```
sudo sshd -T | grep -Ei 'allowusers|allowgroups|denyusers|denygroups'
```

```
ssh -i ~/Baixades/labsuser.pem prova@<IP_PUBLICA> hostname    # ara es rebutja
ssh -i ~/Baixades/labsuser.pem ubuntu@<IP_PUBLICA> hostname   # continua
funcionant
```

Al registre del servidor queda constància del motiu:

```
sudo journalctl -u ssh -n 20
# ... User prova from <IP> not allowed because none of user's groups are
listed in AllowGroups
```

Perill

No us quedeu fora. Si restringiu l'accés i l'usuari `ubuntu` no hi compleix, perdreu l'accés SSH a la instància. Abans d'aplicar canvis:

- Mantingueu **oberta** una sessió SSH (i el túnel de Webmin) mentre proveu des d'un terminal nou.
- Comproveu que `ubuntu` pertany al grup: `id ubuntu`.
- Si alguna cosa falla, desfeu el canvi des de la sessió que teniu oberta o des de Webmin.

6. Tancar

- Tanqueu el túnel amb `Ctrl` + `C` al terminal on l'heu obert.
- Si no l'heu de reutilitzar, elimineu l'usuari de prova: `sudo deluser --remove-home prova`.
- Recordeu que, en aturar el laboratori d'AWS Academy, la IP pública de la instància canvia.

Per a saber-ne més

- Webmin — descàrrega i instal·lació
- Webmin — mòdul SSH Server
- OpenSSH — `ssh` (opcions `-L`, `-N`)
- OpenSSH — `sshd_config` (`AllowUsers`, `AllowGroups`, `PasswordAuthentication`…)
- Ubuntu Server — OpenSSH server
- AWS — Grups de seguretat d'Amazon EC2