2. El servidor SSH

Fitxers i responsabilitats

El servidor OpenSSH és el procés `sshd`. La configuració principal es guarda en el fitxer `sshd_config`, dins del directori de configuració d'OpenSSH. La directiva `Include` permet incorporar fitxers addicionals del subdirectori `sshd_config.d`.

En Ubuntu, es pot consultar l'estat amb `systemctl status ssh`. Algunes instal·lacions utilitzen també `ssh.socket` per a activar el servei sota demanda; cal comprovar les unitats presents si es modifica el port d'escolta.

Opcions principals

Els valors següents expliquen la sintaxi; no representen necessàriament els valors predeterminats de tots els sistemes.

Directiva	Valors o exemple	Funció
`Port`	`22`	Port d'escolta
`PermitRootLogin`	`yes`, `no`, `prohibit-password`, `forced-commands-only`	Condicions d'accés directe de root
`PasswordAuthentication`	`yes` / `no`	Autenticació per contrasenya
`PubkeyAuthentication`	`yes` / `no`	Autenticació amb clau pública
`AllowUsers`	`alumne professor`	Usuaris autoritzats
`AllowTcpForwarding`	`yes`, `no`, `local`, `remote`	Permís de redirecció TCP
`AllowAgentForwarding`	`yes` / `no`	Permís de reenviament de l'agent

Directiva	Valors o exemple	Funció
`X11Forwarding`	`yes` / `no`	Permís de redirecció X11
`ClientAliveInterval`	`60`	Interval en segons de les comprovacions de resposta del client
`ClientAliveCountMax`	`3`	Llindar de comprovacions sense resposta abans de desconnectar
`LogLevel`	`QUIET`, `FATAL`, `ERROR`, `INFO`, `VERBOSE`, `DEBUG`, `DEBUG1`, `DEBUG2`, `DEBUG3`	Detall dels registres

Les comprovacions `ClientAlive*` detecten clients que no responen; no equivalen a mesurar quant de temps fa que una persona no tecleja.

Exemple de configuració

```
PermitRootLogin no
PubkeyAuthentication yes
PasswordAuthentication yes
AllowTcpForwarding yes
AllowAgentForwarding no
ClientAliveInterval 60
ClientAliveCountMax 3
LogLevel INFO
```

En un entorn basat en claus es pot passar `PasswordAuthentication` a `no` després de verificar l'accés. Si també hi ha autenticació interactiva amb PAM, s'ha de revisar `KbdInteractiveAuthentication`.

Aplicar canvis i diagnosticar

Abans de recarregar el servei, es valida la sintaxi:

```
sudo sshd -t
sudo sshd -T
sudo systemctl reload ssh
sudo systemctl status ssh
sudo ss -ltnp
sudo journalctl -u ssh -n 50 --no-pager
```

`sshd -t` comprova la configuració; `sshd -T` mostra els valors efectius generals. Les regles `Match` poden requerir consultar un context de connexió concret amb `-C`. En OpenSSH, l'ordre de les directives i els fitxers inclosos importa: no s'ha de suposar que l'última línia preval.

El reinici amb `sudo systemctl restart ssh` també és possible. Es manté oberta la sessió actual mentre es comprova una connexió nova. Un canvi de port exigix revisar igualment el tallafocs i, si correspon, `ssh.socket`.

Referències

- Manual de sshd_config.
- Manual de sshd: validació i configuració efectiva.
- Ubuntu Server: OpenSSH.