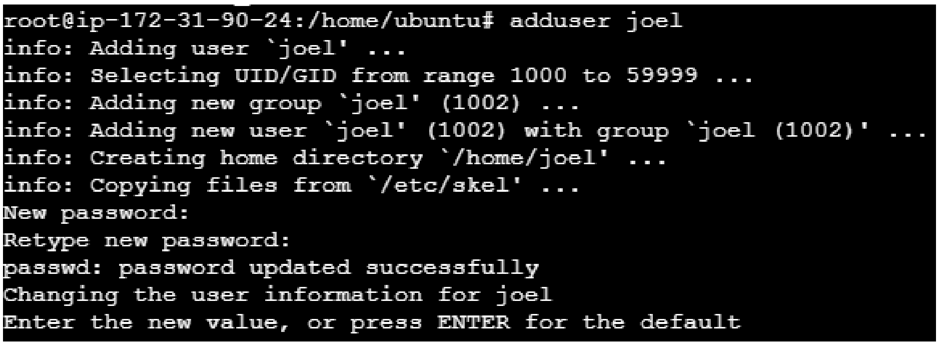
PROJECTE M12 LINKEDIN

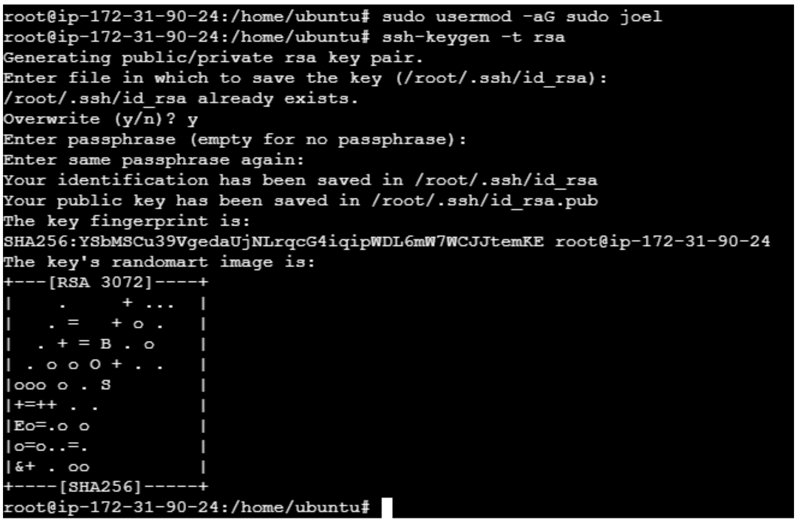
Configuració servidor SSH

creació d'usuari SSH



```
root@ip-172-31-90-24:/home/ubuntu# adduser joel
info: Adding user `joel' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `joel' (1002) ...
info: Adding new user `joel' (1002) with group `joel (1002)' ...
info: Creating home directory `/home/joel' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for joel
Enter the new value, or press ENTER for the default
```

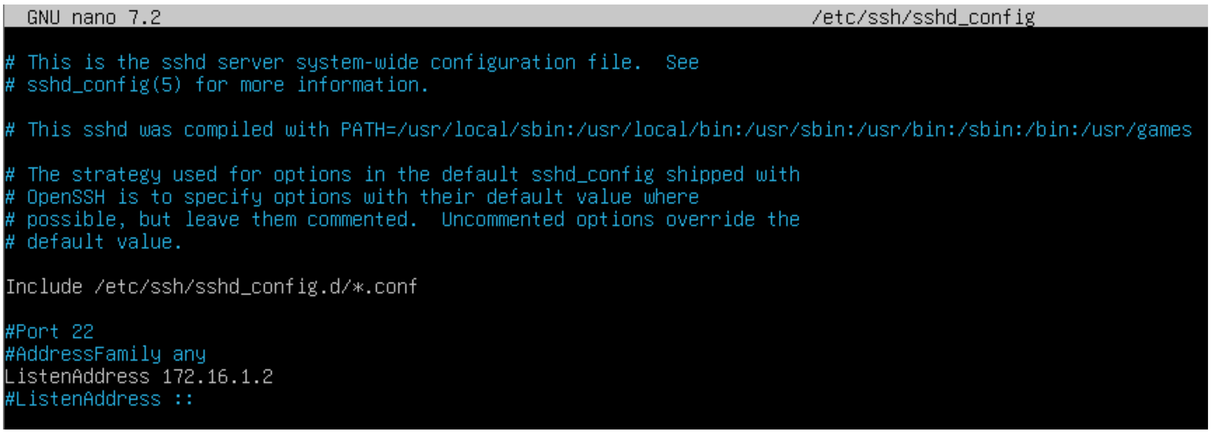
Generem claus rsa



```
root@ip-172-31-90-24:/home/ubuntu# sudo usermod -aG sudo joel
root@ip-172-31-90-24:/home/ubuntu# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:YSbMSCu39VgedaUjNLrqcG4iqipWDL6mW7WCJJtemKE root@ip-172-31-90-24
The key's randomart image is:
+---[RSA 3072]----+
|    .     + ...  |
|   . =   + o .   |
|  . + = B . o    |
| . o o O + . .   |
|ooo o . S        |
|+=++ . .         |
|Eo=.o o          |
|o=o..=.          |
|&+ . oo          |
+----[SHA256]-----+
root@ip-172-31-90-24:/home/ubuntu#
```

Fitxer de configuració SSH

Deshabilitarem la connexió per contrasenya solament per claus i solament es podran connectar els usuaris del mateix rang IP

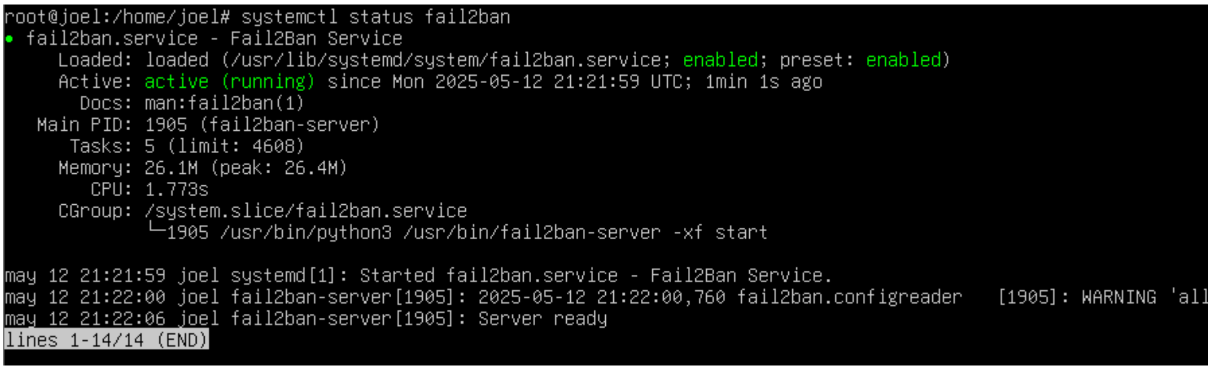


```
  GNU nano 7.2                                                                 /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
ListenAddress 172.16.1.2
#ListenAddress ::
```

fail2ban

"Fail2ban és una eina que se sol utilitzar contra atacs de força bruta al servidor Linux bloquejant IP de manera temporal o permanent".

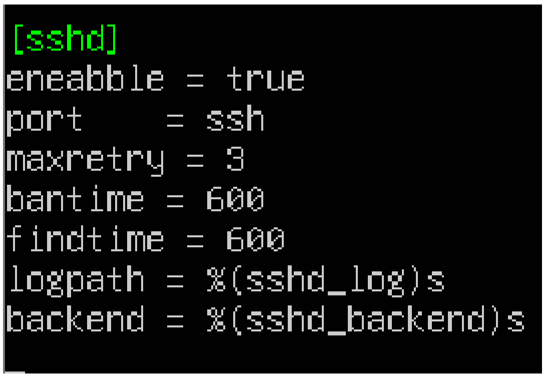
Instal·lem fail2ban



```
root@joel:/home/joel# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-05-12 21:21:59 UTC; 1min 1s ago
       Docs: man:fail2ban(1)
   Main PID: 1905 (fail2ban-server)
      Tasks: 5 (limit: 4608)
     Memory: 26.1M (peak: 26.4M)
        CPU: 1.773s
     CGroup: /system.slice/fail2ban.service
             └─1905 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

may 12 21:21:59 joel systemd[1]: Started fail2ban.service - Fail2Ban Service.
may 12 21:22:00 joel fail2ban-server[1905]: 2025-05-12 21:22:00,760 fail2ban.configreader   [1905]: WARNING 'all
may 12 21:22:06 joel fail2ban-server[1905]: Server ready
lines 1-14/14 (END)
```

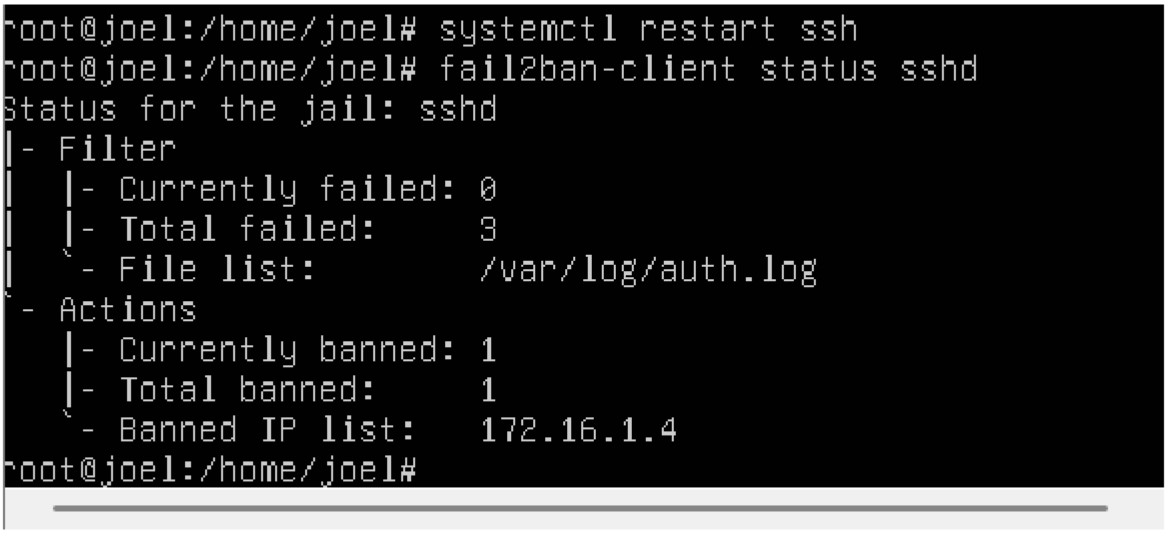
Nosaltres farem servir l'eina per millorar la seguretat per SSH

amb aquesta informació si un usuari falla tres intents de connexió estarà vetat 10 minuts del servidor.

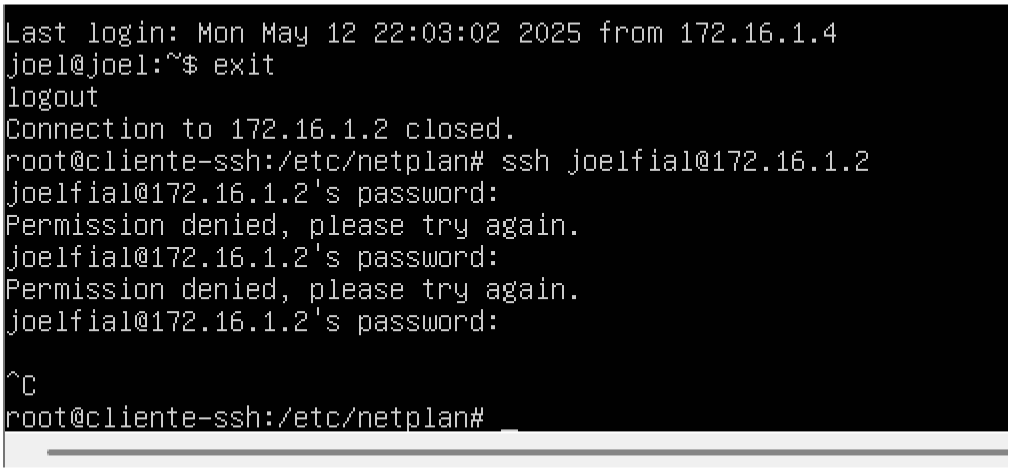


```
[sshd]
eneabble = true
port     = ssh
maxretry = 3
bantime  = 600
findtime = 600
logpath  = %(sshd_log)s
backend  = %(sshd_backend)s
```

Funcionament de la regla



```
root@joel:/home/joel# systemctl restart ssh
root@joel:/home/joel# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     3
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   172.16.1.4
root@joel:/home/joel#
```

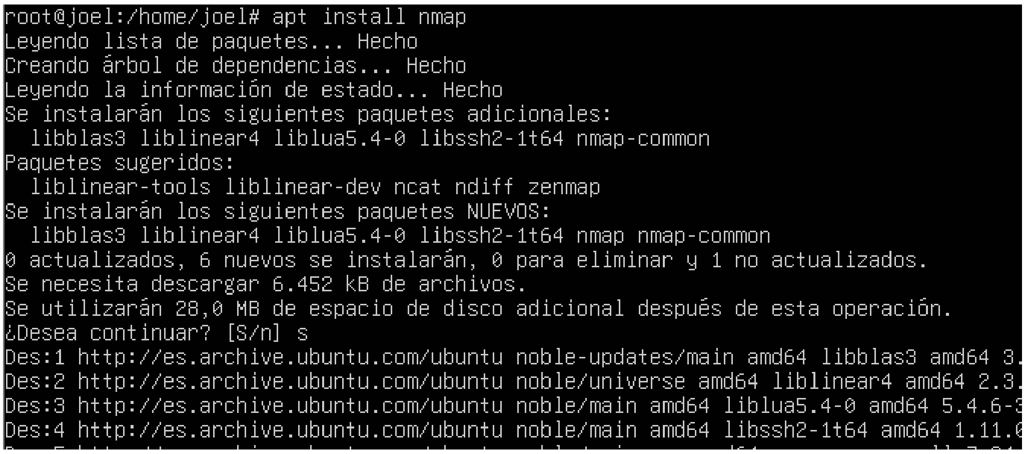


```
Last login: Mon May 12 22:03:02 2025 from 172.16.1.4
joel@joel:~$ exit
logout
Connection to 172.16.1.2 closed.
root@cliente-ssh:/etc/netplan# ssh joelfial@172.16.1.2
joelfial@172.16.1.2's password:
Permission denied, please try again.
joelfial@172.16.1.2's password:
Permission denied, please try again.
joelfial@172.16.1.2's password:

^C
root@cliente-ssh:/etc/netplan# _
```

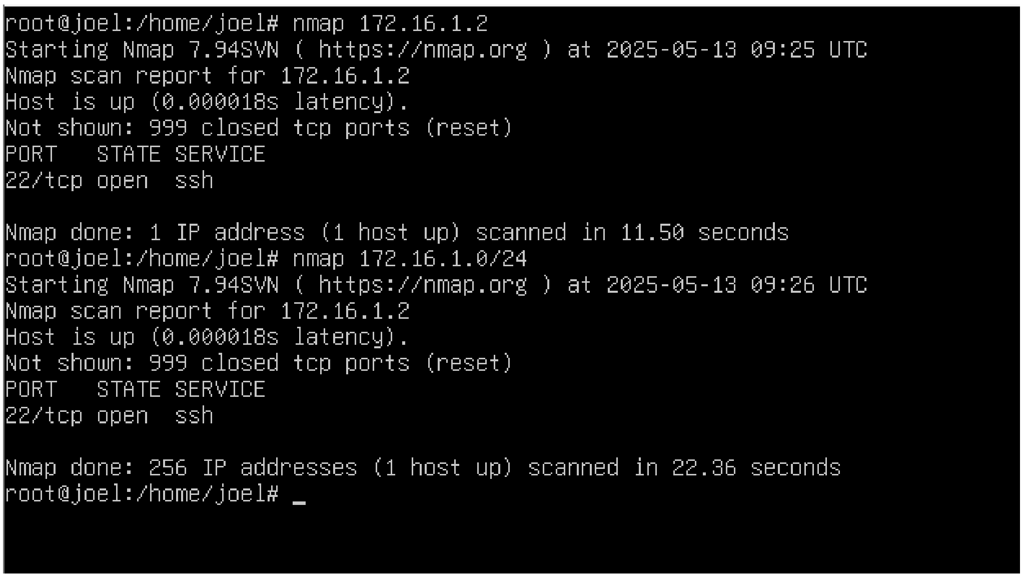
RMIAS DEL SERVIDOR

1. Avaluem els riscos

   Per poder identificar amenaces al servidor instal·lem l'eina nmap



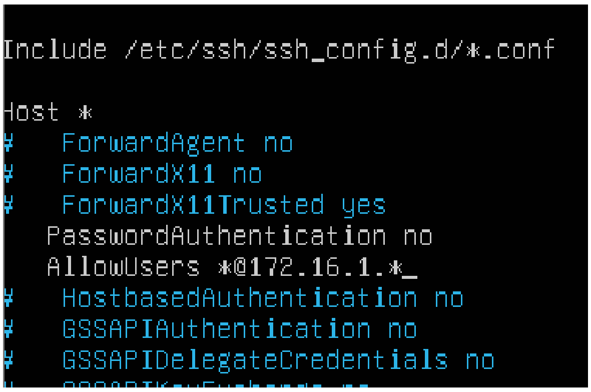
```
root@joel:/home/joel# apt install nmap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap-common
Paquetes sugeridos:
  liblinear-tools liblinear-dev ncat ndiff zenmap
Se instalarán los siguientes paquetes NUEVOS:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap nmap-common
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 1 no actualizados.
Se necesita descargar 6.452 kB de archivos.
Se utilizarán 28,0 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 libblas3 amd64 3.
Des:2 http://es.archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3.
Des:3 http://es.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3
Des:4 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.0
```



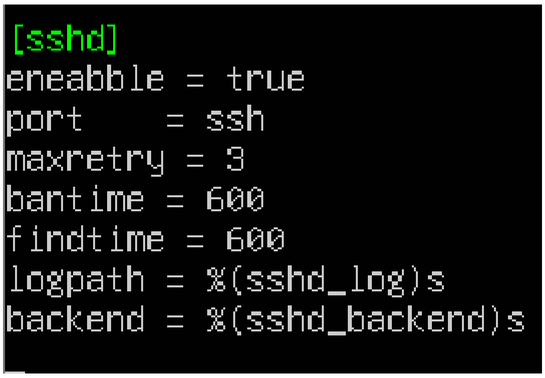
```
root@joel:/home/joel# nmap 172.16.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 09:25 UTC
Nmap scan report for 172.16.1.2
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
root@joel:/home/joel# nmap 172.16.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 09:26 UTC
Nmap scan report for 172.16.1.2
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (1 host up) scanned in 22.36 seconds
root@joel:/home/joel# _
```

2. Control d'accés

Hem implementat a la configuració de SSH que no es pot accedir per contrasenya sinó amb les keys rsa i solament amb , també amb l'eina de Fail2ban el ban de les IP de l'accés no autoritzat.



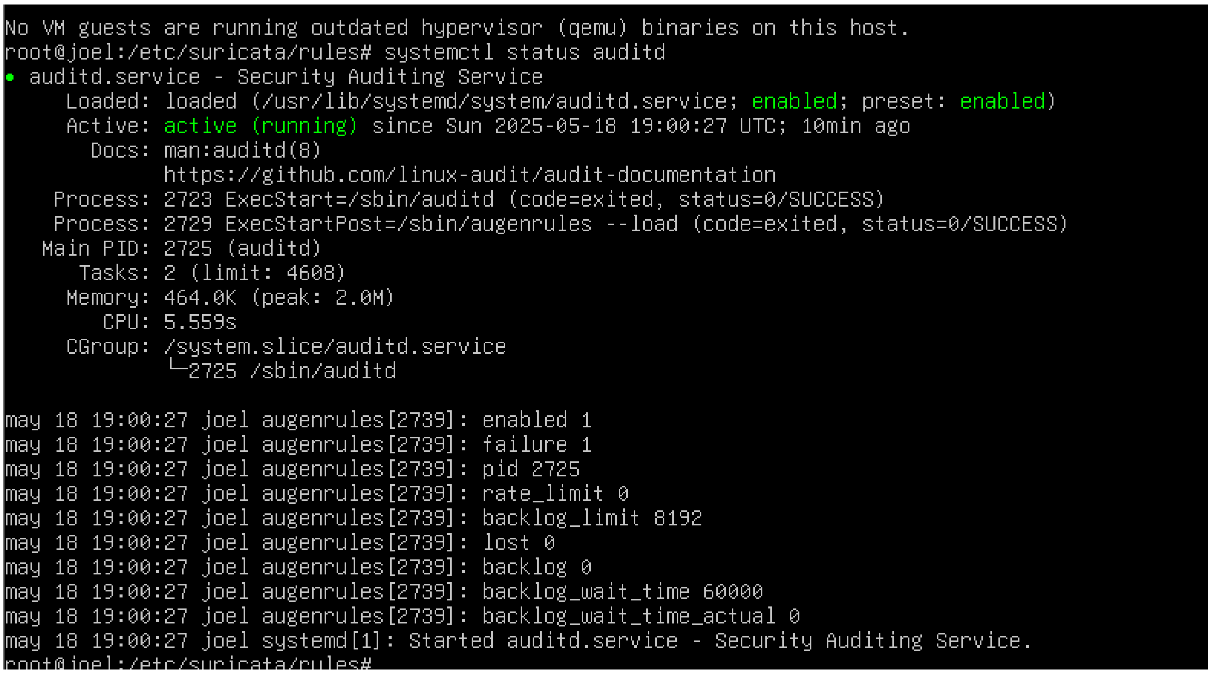
```
Include /etc/ssh/ssh_config.d/*.conf

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
   PasswordAuthentication no
   AllowUsers *@172.16.1.*_
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
```



```
[sshd]
eneabble = true
port     = ssh
maxretry = 3
bantime = 600
findtime = 600
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

3. Monitoratge d'intrusos al servidor

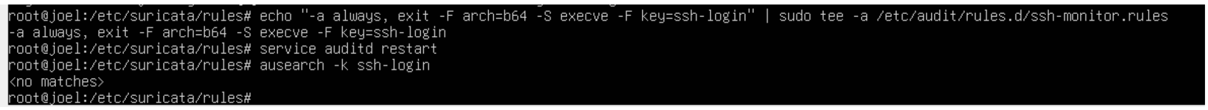
Per poder aconseguir el monitoratge a temps real utilitzaré l'eina de AuditD aquesta eina analitza i detecta a la xarxa del servidor



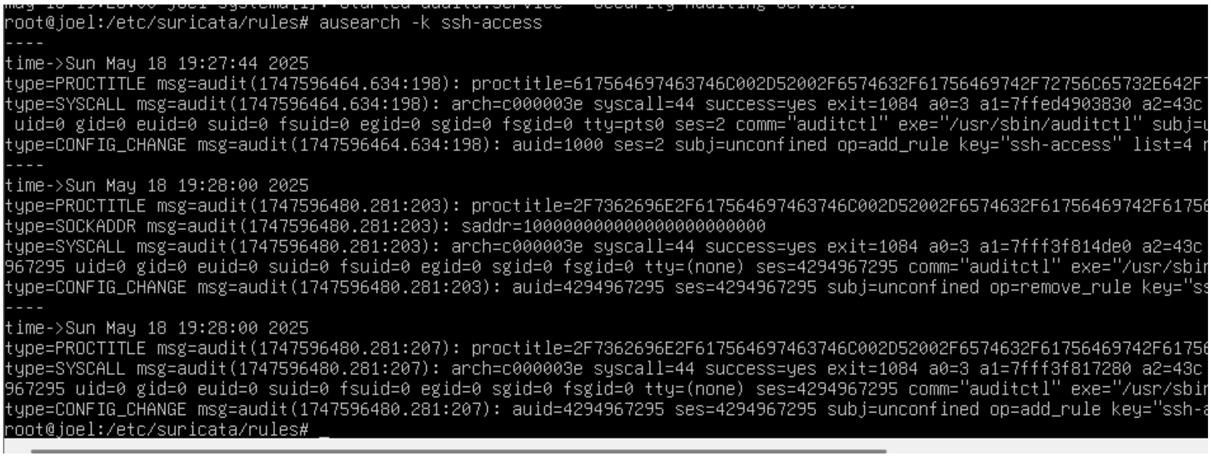
```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@joel:/etc/suricata/rules# systemctl status auditd
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-05-18 19:00:27 UTC; 10min ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
    Process: 2723 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
    Process: 2729 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
   Main PID: 2725 (auditd)
      Tasks: 2 (limit: 4608)
     Memory: 464.0K (peak: 2.0M)
        CPU: 5.559s
     CGroup: /system.slice/auditd.service
             └─2725 /sbin/auditd

may 18 19:00:27 joel augenrules[2739]: enabled 1
may 18 19:00:27 joel augenrules[2739]: failure 1
may 18 19:00:27 joel augenrules[2739]: pid 2725
may 18 19:00:27 joel augenrules[2739]: rate_limit 0
may 18 19:00:27 joel augenrules[2739]: backlog_limit 8192
may 18 19:00:27 joel augenrules[2739]: lost 0
may 18 19:00:27 joel augenrules[2739]: backlog 0
may 18 19:00:27 joel augenrules[2739]: backlog_wait_time 60000
may 18 19:00:27 joel augenrules[2739]: backlog_wait_time_actual 0
may 18 19:00:27 joel systemd[1]: Started auditd.service - Security Auditing Service.
root@joel:/etc/suricata/rules#
```

Configuració de AuditD

Cuando un usuari intenta iniciar sessió en el servidor (exitosa o fallida), AuditD captura el moment d'inici de sessió i s'executa execve para SSH



```
root@joel:/etc/suricata/rules# echo "-a always, exit -F arch=b64 -S execve -F key=ssh-login" | sudo tee -a /etc/audit/rules.d/ssh-monitor.rules
-a always, exit -F arch=b64 -S execve -F key=ssh-login
root@joel:/etc/suricata/rules# service auditd restart
root@joel:/etc/suricata/rules# ausearch -k ssh-login
<no matches>
root@joel:/etc/suricata/rules#
```

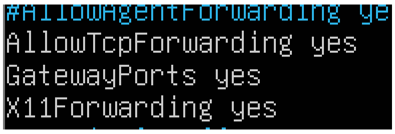


```
May 18 19:28:00 joel systemd[1]: Started auditd.service - Security Auditing Service.
root@joel:/etc/suricata/rules# ausearch -k ssh-access
----
time->Sun May 18 19:27:44 2025
type=PROCTITLE msg=audit(1747596464.634:198): proctitle=617564697463746C002D52002F6574632F61756469742F72756C65732E642F
type=SYSCALL msg=audit(1747596464.634:198): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7ffed4903830 a2=43c
 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=2 comm="auditctl" exe="/usr/sbin/auditctl" subj=u
type=CONFIG_CHANGE msg=audit(1747596464.634:198): auid=1000 ses=2 subj=unconfined op=add_rule key="ssh-access" list=4 r
----
time->Sun May 18 19:28:00 2025
type=PROCTITLE msg=audit(1747596480.281:203): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F6175
type=SOCKADDR msg=audit(1747596480.281:203): saddr=100000000000000000000000
type=SYSCALL msg=audit(1747596480.281:203): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7fff3f814de0 a2=43c
967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin
type=CONFIG_CHANGE msg=audit(1747596480.281:203): auid=4294967295 ses=4294967295 subj=unconfined op=remove_rule key="ss
----
time->Sun May 18 19:28:00 2025
type=PROCTITLE msg=audit(1747596480.281:207): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F6175
type=SYSCALL msg=audit(1747596480.281:207): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7fff3f817280 a2=43c
967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin
type=CONFIG_CHANGE msg=audit(1747596480.281:207): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="ssh-a
root@joel:/etc/suricata/rules# _
```

Túnels SSH

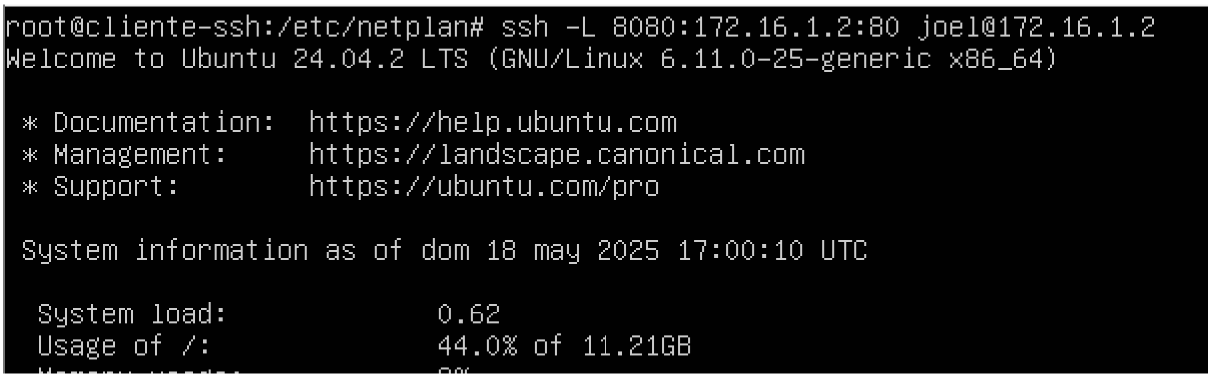
amb els túnels SSH podrem redirigir la connexió remota amb SSH i poder navegar de forma més segura sense exposar-lo públicament

Configurem a SSH l'activació dels ports



```
#AllowAgentForwarding ye
AllowTcpForwarding yes
GatewayPorts yes
X11Forwarding yes
```

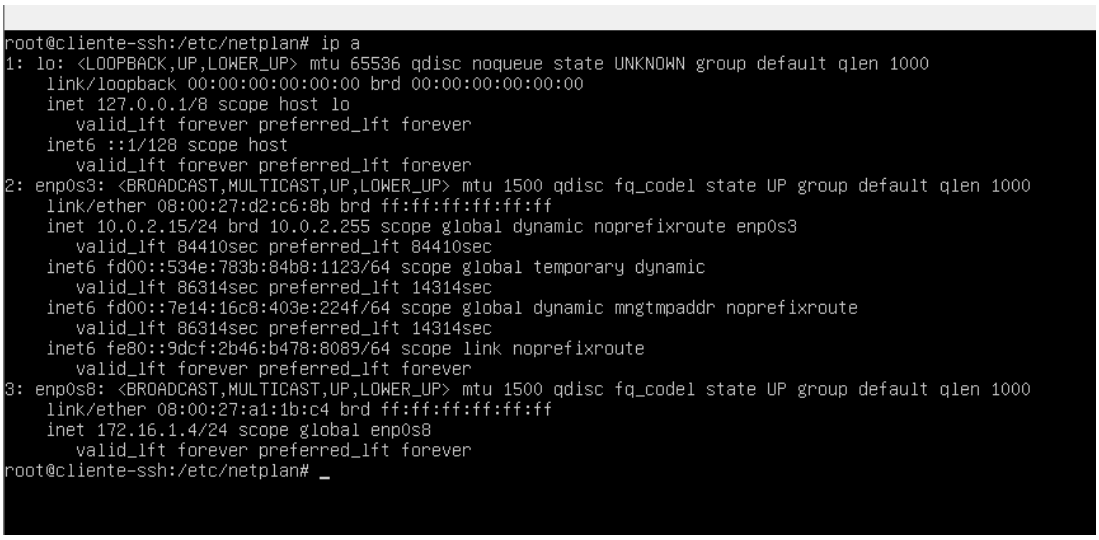
creem un tunel SSH



```
root@cliente-ssh:/etc/netplan# ssh -L 8080:172.16.1.2:80 joel@172.16.1.2
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of dom 18 may 2025 17:00:10 UTC

  System load:             0.62
  Usage of /:              44.0% of 11.21GB
```

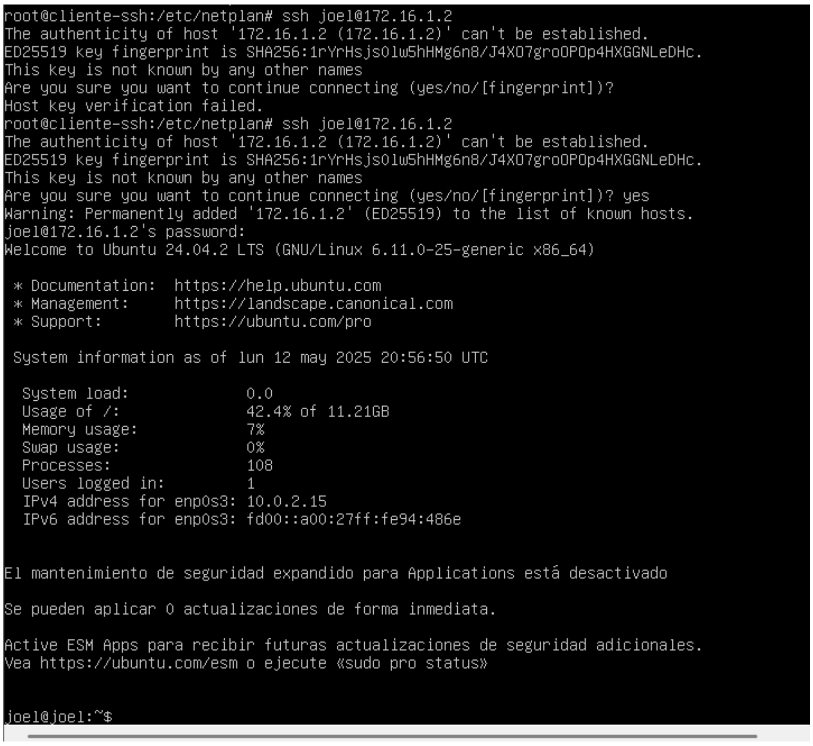
CLIENT

configurem l’interfície del client



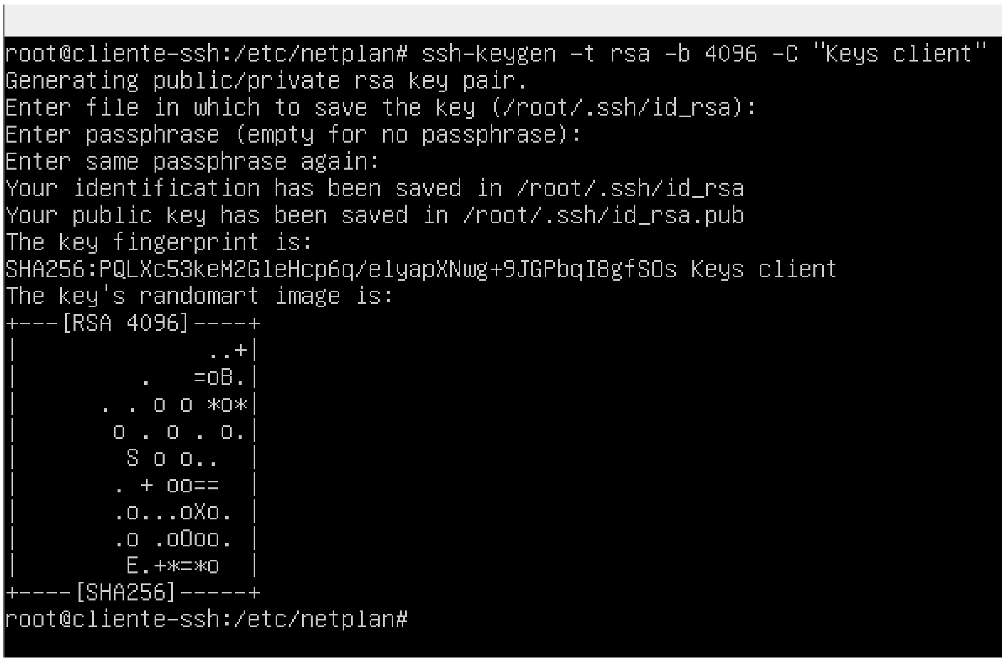
```
root@cliente-ssh:/etc/netplan# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d2:c6:8b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 84410sec preferred_lft 84410sec
    inet6 fd00::534e:783b:84b8:1123/64 scope global temporary dynamic
       valid_lft 86314sec preferred_lft 14314sec
    inet6 fd00::7e14:16c8:403e:224f/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86314sec preferred_lft 14314sec
    inet6 fe80::9dcf:2b46:b478:8089/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a1:1b:c4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.4/24 scope global enp0s8
       valid_lft forever preferred_lft forever
root@cliente-ssh:/etc/netplan# _
```

comprovem si hi ha connexió per SSH



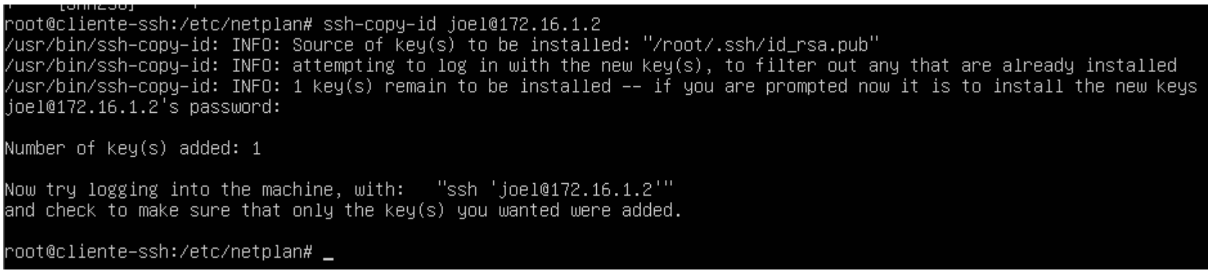
```
root@cliente-ssh:/etc/netplan# ssh joel@172.16.1.2
The authenticity of host '172.16.1.2 (172.16.1.2)' can't be established.
ED25519 key fingerprint is SHA256:1rYrHsjs0lw5hHMg6n8/J4X07groOPOp4HXGGNLeDHc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
root@cliente-ssh:/etc/netplan# ssh joel@172.16.1.2
The authenticity of host '172.16.1.2 (172.16.1.2)' can't be established.
ED25519 key fingerprint is SHA256:1rYrHsjs0lw5hHMg6n8/J4X07groOPOp4HXGGNLeDHc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.1.2' (ED25519) to the list of known hosts.
joel@172.16.1.2's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of lun 12 may 2025 20:56:50 UTC

  System load:             0.0
  Usage of /:              42.4% of 11.21GB
  Memory usage:            7%
  Swap usage:              0%
  Processes:               108
  Users logged in:         1
  IPv4 address for enp0s3: 10.0.2.15
  IPv6 address for enp0s3: fd00::a00:27ff:fe94:486e


El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


joel@joel:~$
```

Generem dos claus rsa al client s’ha generat una keys pública que serà per al servidor i una keys privada.



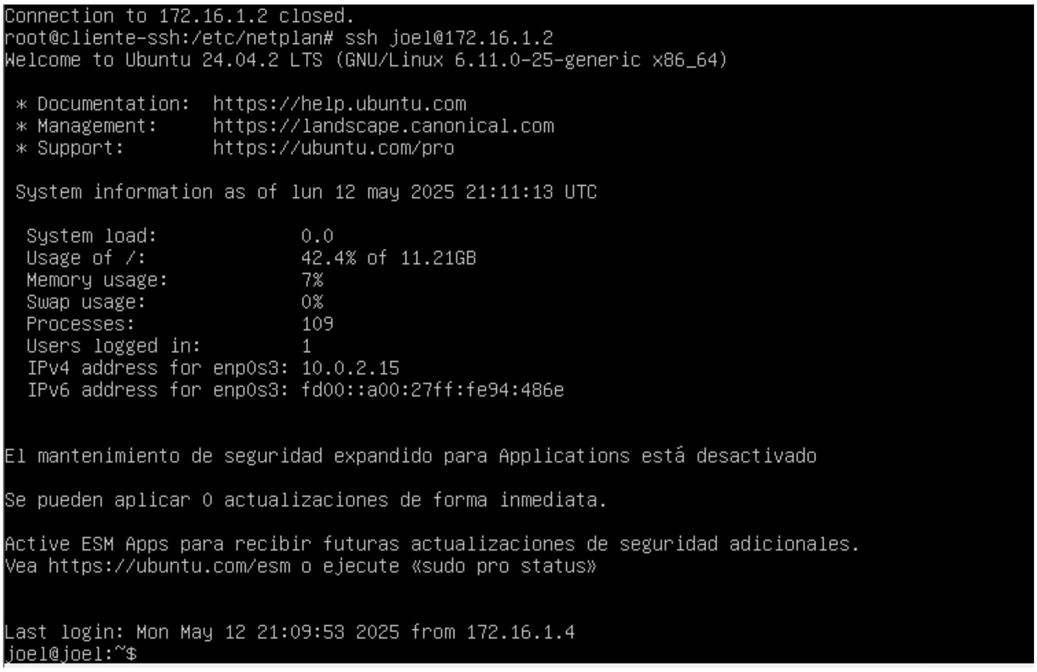
```
root@cliente-ssh:/etc/netplan# ssh-keygen -t rsa -b 4096 -C "Keys client"
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:PQLXc53keM2GleHcp6q/elyapXNwg+9JGPbqI8gfSOs Keys client
The key's randomart image is:
+---[RSA 4096]----+
|              ..+|
|         .   =oB.|
|      . . o o *o*|
|       o . o . o.|
|        S o o..  |
|       . + oo==  |
|       .o...oXo. |
|       .o .oOoo. |
|        E.+*=*o  |
+----[SHA256]-----+
root@cliente-ssh:/etc/netplan#
```

Per via SSH enviarem la nostra clau pública al servidor per poder registrar-nos sense contrasenya



```
root@cliente-ssh:/etc/netplan# ssh-copy-id joel@172.16.1.2
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
joel@172.16.1.2's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'joel@172.16.1.2'"
and check to make sure that only the key(s) you wanted were added.

root@cliente-ssh:/etc/netplan# _
```

Connexió de client a servidor SSH



```
Connection to 172.16.1.2 closed.
root@cliente-ssh:/etc/netplan# ssh joel@172.16.1.2
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of lun 12 may 2025 21:11:13 UTC

  System load:            0.0
  Usage of /:             42.4% of 11.21GB
  Memory usage:           7%
  Swap usage:             0%
  Processes:              109
  Users logged in:        1
  IPv4 address for enp0s3: 10.0.2.15
  IPv6 address for enp0s3: fd00::a00:27ff:fe94:486e


El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


Last login: Mon May 12 21:09:53 2025 from 172.16.1.4
joel@joel:~$
```

Vídeo demostració

ENLLAÇ

CONCLUSIÓ

Gràcies amb aquest projecte he après estratègies de seguretat com RMIAS nou coneixements de Linux i servidors SSH