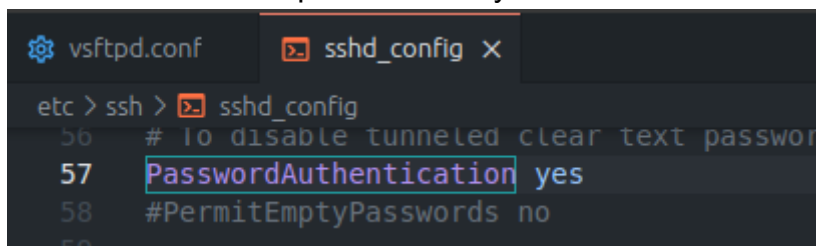


Ejercicio 1

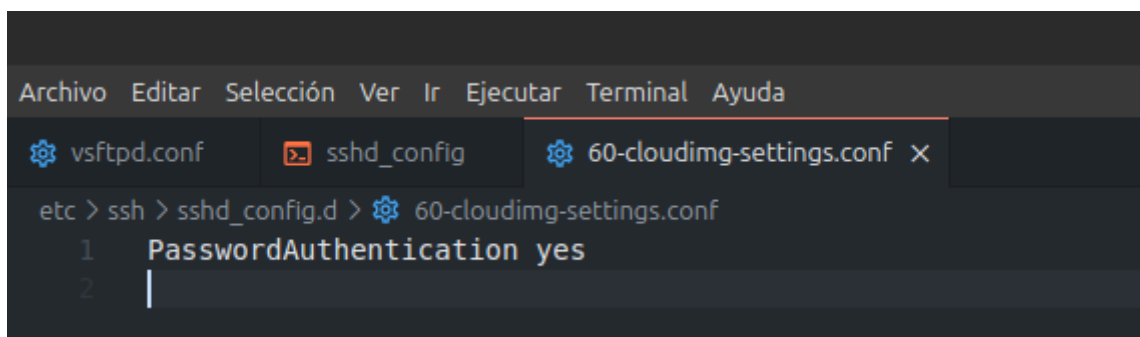
Crea al servidor remot un nou usuari xyyyy on x és el teu nom e yyyy el teu cognom en el servidor.

```
• root@ip-172-31-41-232:/# sudo adduser pguill
info: Adding user `pguill' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `pguill' (1002) ...
info: Adding new user `pguill' (1002) with group `pguill (1002)' ...
info: Creating home directory `/home/pguill' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for pguill
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
info: Adding new user `pguill' to supplemental / extra groups `users' ...
info: Adding user `pguill' to group `users' ...
```

- Activa l'autenticació per contrasenya



```
etc > ssh > sshd_config
56 # To disable tunneled clear text passwords
57 PasswordAuthentication yes
58 #PermitEmptyPasswords no
59
```



```
Archivo Editar Selección Ver Ir Ejecutar Terminal Ayuda
etc > ssh > sshd_config.d > 60-cloudimg-settings.conf
1 PasswordAuthentication yes
2 |
```

- Connecta't des de la màquina local al servidor utilitzant la contrasenya d'aquest nou usuari.

```

batoi@batoi-SSD-2024:~/Documentos/DAW 2/Desarrollo WEB en cliente/Ej 2.1/librosbatoi$ ssh pguill@54.81.47.114
pguill@54.81.47.114's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1017-aws x86_64)

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

System information as of Wed Oct 30 16:54:42 UTC 2024

System load:  0.0           Processes:      130
Usage of /:   41.5% of 6.71GB Users logged in:  0
Memory usage: 54%          IPv4 address for enX0: 172.31.41.232
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

108 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

```

- Comprova que tens accés al servidor i que pots utilitzar-lo.

```

pguill@ip-172-31-41-232:~$ mkdir hola
pguill@ip-172-31-41-232:~$ ls -rl
total 4
drwxrwxr-x 2 pguill pguill 4096 Oct 30 16:55 hola

```

Ejercicio 2

Du a terme les següents tasques:

- Genera un nou usuari a la màquina remota

```

● root@ip-172-31-41-232:/# sudo adduser pedro
info: Adding user `pedro' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `pedro' (1003) ...
info: Adding new user `pedro' (1003) with group `pedro (1003)' ...
info: Creating home directory `/home/pedro' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for pedro
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user `pedro' to supplemental / extra groups `users' ...
info: Adding user `pedro' to group `users' ...

```

- Genera un parell de claus SSH a la màquina local

```

batoi@batoi-SSD-2024:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/batoi/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/batoi/.ssh/id_rsa
Your public key has been saved in /home/batoi/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:bttwPzKFJTt8sZddZpi23Jl0seyV7VsyZkmwL0+YoF0 batoi@batoi-SSD-2024
The key's randomart image is:
+---[RSA 4096]---+
|                 |
|      . .        |
|    . 0.0=       |
|   o  = ==B      |
|  S. B *oX*      |
| .. E = @+=      |
| o+o.B + oo      |
| ...==.0 .       |
|  . .0..         |
+-----[SHA256]-----+

```

- Copia la clau pública al servidor.

```
cat ~/.ssh/id_rsa.pub | ssh pedro@54.81.47.114 'cat >> ~/.ssh/authorized_k
```

- Habilita l'accés per usuari/contrasenya
Ya esta habilitado de antes.

- Connecta't al servidor utilitzant la teua clau privada, sense contrasenya.

```
batoi@batoi-SSD-2024:~$ ssh pedro@54.81.47.114
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1017-aws x86_64)

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

System information as of Wed Oct 30 17:09:45 UTC 2024

System load:  0.0               Processes:            131
Usage of /:   41.6% of 6.71GB   Users logged in:     0
Memory usage: 52%              IPv4 address for enX0: 172.31.41.232
Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

108 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Oct 30 17:07:46 2024 from 213.0.87.194
```

```

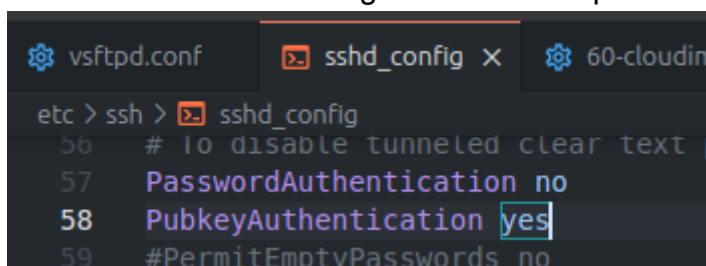
batoi@batoi-SSD-2024:~$ ssh -v pedro@54.81.47.114
OpenSSH_9.6p1 Ubuntu-3ubuntu13.5, OpenSSL 3.0.13 30 Jan 2024
debug1: Reading configuration data /home/batoi/.ssh/config
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 54.81.47.114 [54.81.47.114] port 22.
debug1: Connection established.
debug1: identity file /home/batoi/.ssh/id_rsa type 0
debug1: identity file /home/batoi/.ssh/id_rsa-cert type -1
debug1: identity file /home/batoi/.ssh/id_ecdsa type -1
debug1: identity file /home/batoi/.ssh/id_ecdsa-cert type -1
debug1: identity file /home/batoi/.ssh/id_ecdsa_sk type -1
debug1: identity file /home/batoi/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /home/batoi/.ssh/id_ed25519 type -1
debug1: identity file /home/batoi/.ssh/id_ed25519-cert type -1
debug1: identity file /home/batoi/.ssh/id_ed25519_sk type -1
debug1: identity file /home/batoi/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /home/batoi/.ssh/id_xmss type -1
debug1: identity file /home/batoi/.ssh/id_xmss-cert type -1
debug1: identity file /home/batoi/.ssh/id_dsa type -1
debug1: identity file /home/batoi/.ssh/id_dsa-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.5
debug1: Remote protocol version 2.0, remote software version OpenSSH 9.6p1 Ubuntu-3ubuntu13.4
debug1: compat_banner: match: OpenSSH_9.6p1 Ubuntu-3ubuntu13.4 pat OpenSSH* compat 0x04000000
debug1: Authenticating to 54.81.47.114:22 as 'pedro'
debug1: load_hostkeys: fopen /home/batoi/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: sntrup761x25519-sha512@openssh.com
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:ngbpu2ZeY+QJ0z0ody7qB8uEed2Vmp7g4yB8veTwt+k
debug1: load_hostkeys: fopen /home/batoi/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory

```

Actividad 3

Du a terme les següents tasques:

- Modifica el fitxer de configuració de SSH per desactivar l'autenticació per contrasenya.



```

etc > ssh > sshd_config
56 # To disable tunneled clear text
57 PasswordAuthentication no
58 PubkeyAuthentication yes
59 #PermitEmptyPasswords no

```

- Assegura't que només pots connectar-te al servidor utilitzant la clau privada.

Usuario que tiene la clave privada

```

batoi@batoi-SSD-2024:~$ ssh pedro@54.81.47.114
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1017-aws x86_64)

```

Usuario que no tiene la clave privada

```

batoi@batoi-SSD-2024:~$ ssh pguill@54.81.47.114
pguill@54.81.47.114: Permission denied (publickey).
batoi@batoi-SSD-2024:~$

```

- (opcional) Per augmentar la seguretat canvia el port per defecte en el que el teu servidor ssh escolta les connexions per el port 32002 i connectat fent us d'aquest port.

Usando la regla Port 3002

```
batoi@batoi-SSD-2024:~$ ssh pedro@54.81.47.114 -P 32002  
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1017-aws x86_64)
```