

2º ASIR

Práctica 12

SSH

Administración de sistemas operativos

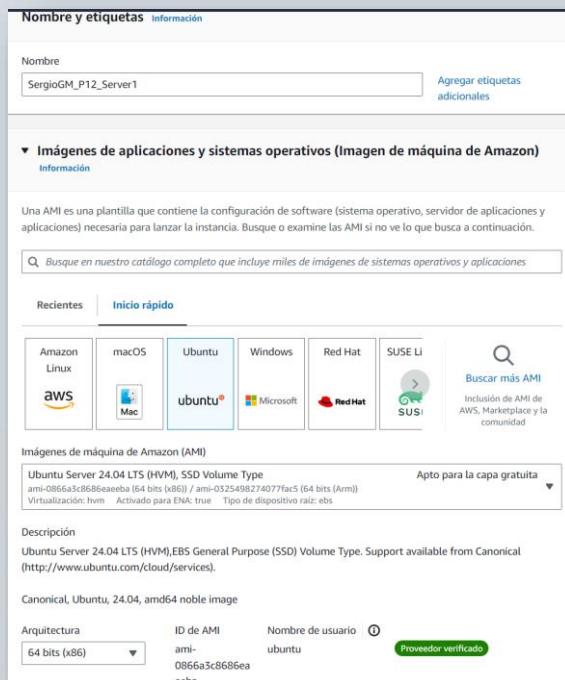
Sergio García Márquez
I.E.S SAN SEBASTIÁN

Índice

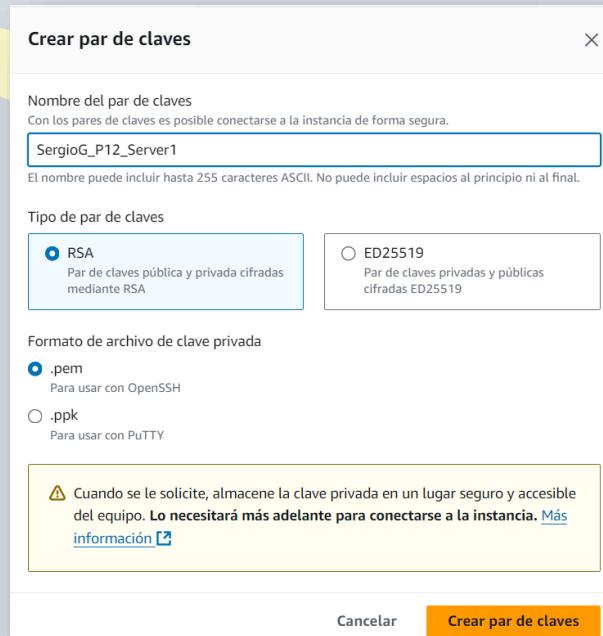
1.	Lanzar servidor Linux con claves nuevas sin contraseña	2
2.	Crear AMI para posibles errores o problemas	7
3.	Configuración del servidor ssh Linux: cambio del puerto	10
4.	Configuración del servidor ssh Linux	12
5.	Generar las claves con el comando keygen.....	15
6.	Lista blanca y negra.....	18
7.	Conexión a servidor Linux sin usar claves criptográficas.....	19
8.	Escritorio remoto.....	20
9.	Crear un túnel ssh para acceso remoto a servicios	25
10.	Tunel con Putty a servidor Web anterior.....	27
11.	Tunel con Putty para conectarse a VNC.....	31
12.	Creación de túnel inverso	35
13.	Transferir archivos desde tu máquina local a la instancia EC2 utilizando SCP..	39
14.	Transferir archivos desde la instancia a tu máquina local a la utilizando SCP ...	40
15.	Subir archivos a un servidor por SSH con WinSCP.....	41
16.	Transferencia de archivos desde Moxterm.....	43
17.	Transferir archivos desde la instancia a tu máquina local a la utilizando SFTP .	46

1. Lanzar servidor Linux con claves nuevas sin contraseña

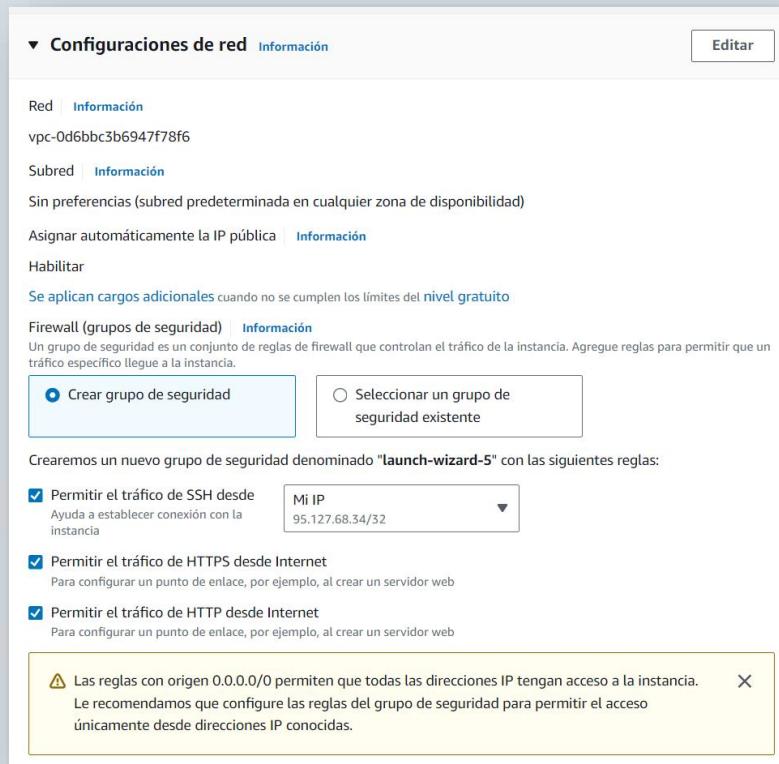
El primer paso será crear un servidor de Ubuntu con las siguientes especificaciones:



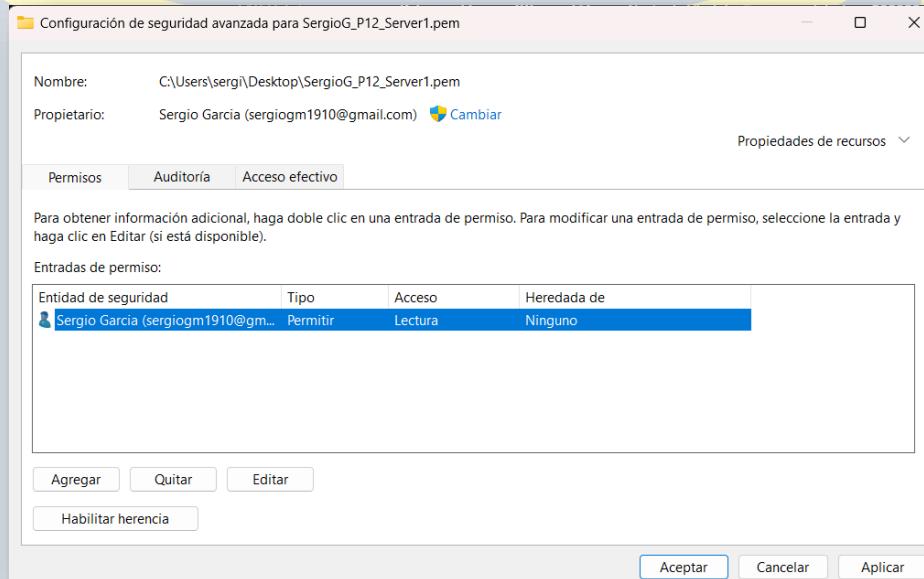
Crearemos un nuevo par de claves que nos descargará el archivo .pem.



Crearemos un grupo de seguridad que permita el ssh y podemos poner nuestra IP para las conexiones ssh para mayor seguridad.



Ahora nos iremos al archivo “.pem”, nos vamos a Propiedades-> seguridad-> avanzadas -> Deshabilitamos la herencia. Quitamos todos los usuarios y nos ponemos permiso de lectura.



Nos vamos a la conexión por ssh y copiamos el comando para mayor comodidad.

The screenshot shows the AWS CloudWatch Metrics interface with the 'Cliente SSH' tab selected. It provides instructions for connecting via SSH:

1. Abra un cliente SSH.
2. Localice el archivo de clave privada. La clave utilizada para lanzar esta instancia es SergioG_P12_Server1.pem
3. Ejecute este comando, si es necesario, para garantizar que la clave no se pueda ver públicamente.
chmod 400 "SergioG_P12_Server1.pem"
4. Conéctese a la instancia mediante su DNS público:
ec2-3-84-61-146.compute-1.amazonaws.com

Ejemplo:
ssh -i "SergioG_P12_Server1.pem" ubuntu@ec2-3-84-61-146.compute-1.amazonaws.com

Nota: En la mayoría de los casos, el nombre de usuario adivinado es correcto. Sin embargo, lea las instrucciones de uso de la AMI para comprobar si el propietario de la AMI ha cambiado el nombre de usuario predeterminado de la AMI.

Sólo queda poner el comando en powershell.

```
PS C:\Users\sergi\Desktop> ssh -i "SergioG_P12_Server1.pem" ubuntu@ec2-3-84-61-146.compute-1.amazonaws.com
The authenticity of host 'ec2-3-84-61-146.compute-1.amazonaws.com (3.84.61.146)' can't be established.
ED25519 key fingerprint is SHA256:dLfM2cwt1CFSzXJbU6YGtL9PpPCtWgFxdRbKSrB/yHk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-84-61-146.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

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

System information as of Tue Oct 22 15:52:32 UTC 2024

System load:  0.12           Processes:          105
Usage of /:   22.9% of 6.71GB  Users logged in:   0
Memory usage: 21%            IPv4 address for enX0: 172.31.86.26
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-86-26:~$ |
```

Ahora le vamos a poner una contraseña al root:

```
root@ip-172-31-86-26:/home> exit
ubuntu@ip-172-31-86-26:~$ sudo su
root@ip-172-31-86-26:/home/ubuntu# sudo root passwd
sudo: root: command not found
root@ip-172-31-86-26:/home/ubuntu# sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
root@ip-172-31-86-26:/home/ubuntu# |
```

Y finalmente crearemos 3 usuarios con mi nombre.

```
root@ip-172-31-86-26:/home/ubuntu# sudo adduser sergio1
info: Adding user `sergio1' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `sergio1' (1001) ...
info: Adding new user `sergio1' (1001) with group `sergio1 (1001)' ...
info: Creating home directory `/home-sergio1' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sergio1
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 `sergio1' to supplemental / extra groups `users' ...
info: Adding user `sergio1' to group `users' ...
root@ip-172-31-86-26:/home/ubuntu# |
```

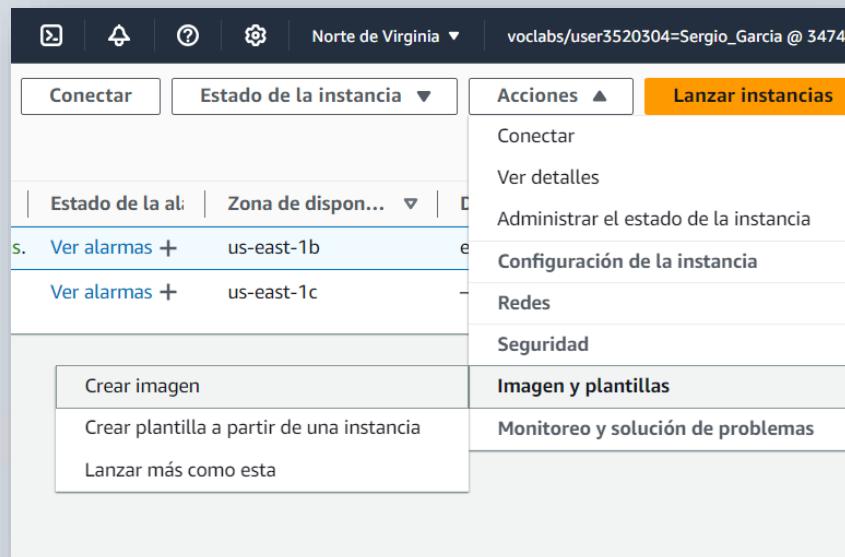
```
root@ip-172-31-86-26:/home# sudo adduser sergio1
info: Adding user 'sergio1' to group 'users' ...
root@ip-172-31-86-26:/home/ubuntu# sudo adduser sergio2
info: Adding user 'sergio2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'sergio2' (1002) ...
info: Adding new user 'sergio2' (1002) with group 'sergio2 (1002)' ...
info: Creating home directory '/home/sergio2' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sergio2
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 'sergio2' to supplemental / extra groups 'users' ...
info: Adding user 'sergio2' to group 'users' ...
root@ip-172-31-86-26:/home/ubuntu# sudo adduser sergio3
info: Adding user 'sergio3' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'sergio3' (1003) ...
info: Adding new user 'sergio3' (1003) with group 'sergio3 (1003)' ...
info: Creating home directory '/home/sergio3' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sergio3
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 'sergio3' to supplemental / extra groups 'users' ...
info: Adding user 'sergio3' to group 'users' ...
root@ip-172-31-86-26:/home/ubuntu# |
```

Con el comando cat /etc/passwd confirmaremos que se crearon.

```
root@ip-172-31-86-26:/home/ubuntu# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
dhpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpd:/bin/false
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin
uuid:x:103:103::/run/uuid:/usr/sbin/nologin
tss:x:104:104:TPM software stack,,,:/var/lib/tpm:/bin/false
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:106:1::/var/cache/pollinate:/bin/false
tcpdump:x:107:108::/nonexistent:/usr/sbin/nologin
landscape:x:108:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/usr/sbin/nologin
ec2-instance-connect:x:109:65534::/nonexistent:/usr/sbin/nologin
_chrony:x:110:112:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
sergio1:x:1001:1001:,,,:/home/sergio1:/bin/bash
sergio2:x:1002:1002:,,,:/home/sergio2:/bin/bash
sergio3:x:1003:1003:,,,:/home/sergio3:/bin/bash
root@ip-172-31-86-26:/home/ubuntu# |
```

2. Crear AMI para posibles errores o problemas

Para crear la imagen, nos iremos a acciones y seleccionamos la opción siguiente:



Y procedemos a crearla con los siguientes datos.

ID de la instancia
i-09d0ebfdd051d61da (SergioGM_P12_Server1)

Nombre de la imagen
SergioGServerSSH

Máximo de 127 caracteres. No se pueden modificar después de su creación.

Descripción de la imagen: *opcional*
Incluye usuarios sertgio1,2,3, ubuntu y root con contraseña

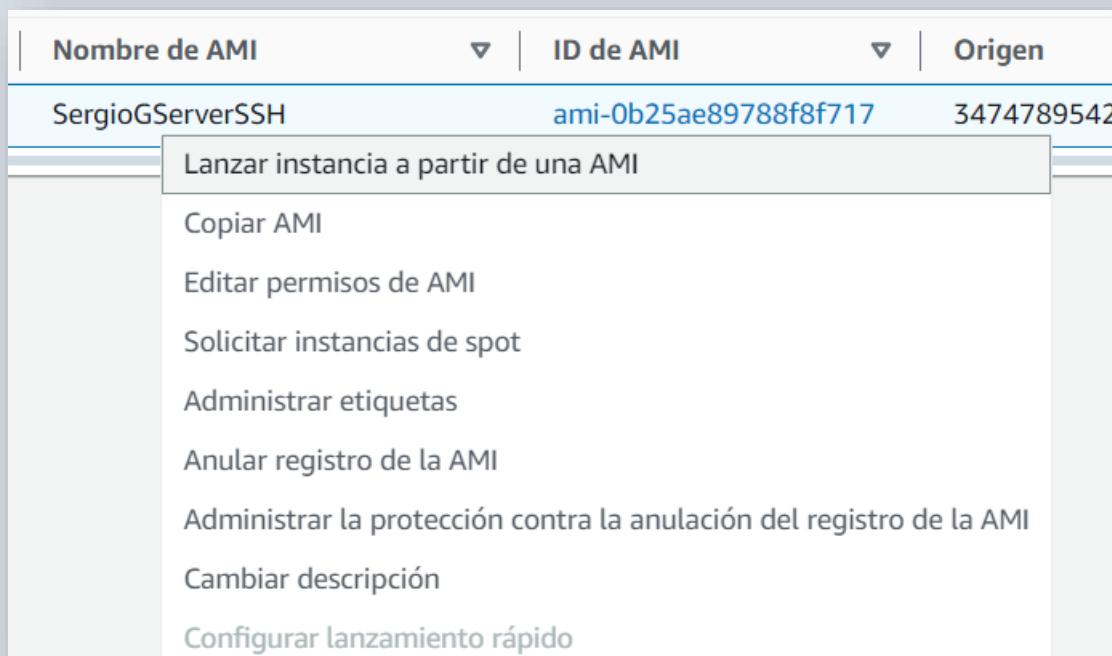
255 caracteres como máximo

Reiniciar instancia
Cuando se selecciona esta opción, Amazon EC2 reinicia la instancia para mantener los datos en reposo cuando se toman instantáneas de los volúmenes asociados. Esto garantiza la coherencia de datos.

Volumenes de instancia

Tipo de almacenamiento	Dispositivo	Instantánea	Tamaño	Tipo de volumen	IOPS	Rendimiento	Eliminar cuando termine	Cifrado
EBS	/...	Crear una nueva...	8	SSD de uso gen...	3000		<input checked="" type="checkbox"/> Habilitar	<input type="checkbox"/> Habilitar

Ya tenemos la AMI, ahora toca lanzar otra instancia a partir de esa imagen. Seleccionamos la imagen y seleccionamos la opción que aparece en pantalla.



Le ponemos nombre y la lanzamos.

Launch an instance Información

Amazon EC2 le permite crear máquinas virtuales, o instancias, que se ejecutan en la nube de AWS. Comience rápidamente siguiendo los sencillos pasos que se indican a continuación.

Nombre y etiquetas Información

Nombre: SergioG_ServerSSH

Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon) Información

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones

AMI del catálogo | Recientes | Mis AMI | Inicio rápido

Nombre: SergioGServerSSH
Descripción: -
ID de imagen: ami-0b25ae89788f8f717
Nombre de usuario: root

Número de instancias Información

1

Imagen de software (AMI)
SergioGServerSSH
ami-0b25ae89788f8f717

Tipo de servidor virtual (tipo de instancia)
t2.micro

Firewall (grupo de seguridad)
Nuevo grupo de seguridad

Almacenamiento (volúmenes)
Volúmenes: 1 (8 GiB)

Nivel gratuito: El primer año incluye 750 horas de uso de instancias t2.micro (o t3.micro en las regiones en las que t2.micro no esté disponible) en las AMI del nivel gratuito al mes, 750 horas de uso de direcciones IPv4 públicas al mes, 30 millones de E/S, 2 millones de E/S, 1 GB de instantáneas y 100 GB de ancho de banda a Internet.

Código de versión preliminar

Ya tenemos lista la instancia a partir de la imagen.

Instancias (1/3) Información									
Buscar Instancia por atributo o etiqueta (case-sensitive)		Todos los e...		Última actualización		Estado de la instancia		Acciones	
Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de estado	Estado de la al.	Zona de dispon...	DNS de IPv4 pública	Direcc...	
<input checked="" type="checkbox"/> SergioG_ServerSSH	i-08908a747941eb0ff	En ejecución	t2.micro	Initializando	Ver alarmas +	us-east-1c	ec2-34-229-138-145.co...	34.229	
<input type="checkbox"/> SergioG_P12_Server1	i-0900ebfd051d61da	En ejecución	t2.micro	2/2 comprobaciones superadas.	Ver alarmas +	us-east-1b	ec2-3-84-61-146.comp...	3.84.6	

Le he asignado la misma clave que cree en la isntancia anterior. Nos iremos al cliente ssh para pegar el comando (y ver que es la misma dirección).

Conexión de la instancia EC2 Administrador de sesiones **Cliente SSH** Consola de serie de EC2

ID de la instancia
 i-08908a747941eb0ff (SergioG_ServerSSH)

1. Abra un cliente SSH.
 2. Localice el archivo de clave privada. La clave utilizada para lanzar esta instancia es SergioG_P12_Server1.pem
 3. Ejecute este comando, si es necesario, para garantizar que la clave no se pueda ver públicamente.
 chmod 400 "SergioG_P12_Server1.pem"
 4. Conéctese a la instancia mediante su DNS público:
 ec2-34-229-138-145.compute-1.amazonaws.com

Comando copiado

ssh -i "SergioG_P12_Server1.pem" root@ec2-34-229-138-145.compute-1.amazonaws.com

Nota: En la mayoría de los casos, el nombre de usuario adivinado es correcto. Sin embargo, lea las instrucciones de uso de la AMI para comprobar si el propietario de la AMI ha cambiado el nombre de usuario predeterminado de la AMI.

```
ubuntu@ip-172-31-30-29:~ % ssh -i "SergioG_P12_Server1.pem" ubuntu@ec2-34-229-138-145.compute-1.amazonaws.com
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

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

System information as of Tue Oct 22 16:10:21 UTC 2024

System load: 0.47      Processes:          107
Usage of /: 23.1% of 6.71GB   Users logged in:    0
Memory usage: 20%           IPv4 address for enX0: 172.31.30.29
Swap usage:  0%           Swap usage:        0

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

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

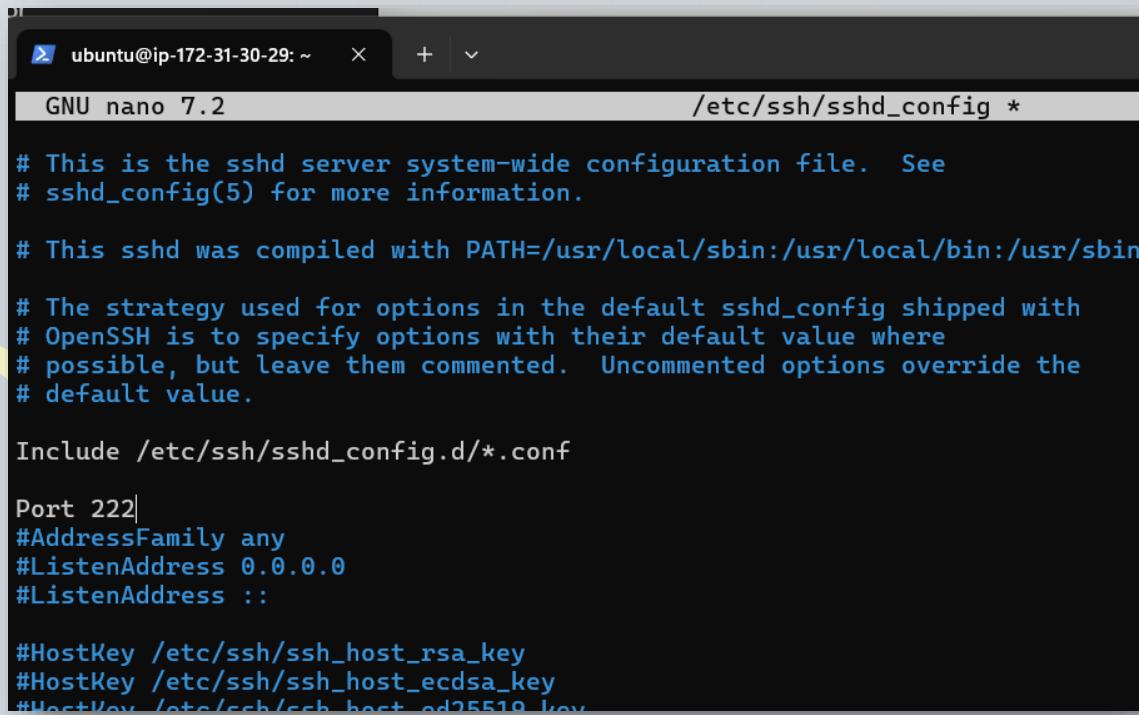
Last login: Tue Oct 22 15:52:34 2024 from 95.127.68.34
ubuntu@ip-172-31-30-29:~ $ |
```

Para finalizar, comprobamos que tenemos creados los mismos usuarios.

```
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
sergio1:x:1001:1001:,:/home/sergio1:/bin/bash
sergio2:x:1002:1002:,:/home/sergio2:/bin/bash
sergio3:x:1003:1003:,:/home/sergio3:/bin/bash
ubuntu@ip-172-31-30-29:~$ |
```

3. Configuración del servidor ssh Linux: cambio del puerto

Cambiaremos el puerto del servidor al puerto 222. Y reiniciaremos el servicio ssh.



```
ubuntu@ip-172-31-30-29: ~ + | 
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

# 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 222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
```

Esto hará que no nos podamos conectar mediante ssh, ya que por defecto escucha por el puerto 22 aws para este tipo de accesos.

Para remediarlo tendremos que acceder al grupo de seguridad y cambiar las reglas de entrada, permitiendo el tráfico TCP por el puerto 222, esto habilitará que escuche por dicho puerto y podamos acceder.

Ahora podremos volver a realizar la conexión mediante ssh por el puerto 222. He verificado que use dicho puerto añadiendo “-p 222” al comando ssh.

```
ubuntu@ip-172-31-30-29: ~ + | 
PS C:\Users\sergi\Desktop> ssh -i "SergioG_P12_Server1.pem" ubuntu@ec2-34-229-138-145.compute-1.amazonaws.com -p 222
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

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

System information as of Tue Oct 22 16:19:46 UTC 2024

System load:  0.2          Processes:           107
Usage of /:   23.2% of 6.71GB  Users logged in:      0
Memory usage: 19%          IPv4 address for enX0: 172.31.30.29
Swap usage:   0%         

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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: Tue Oct 22 16:13:21 2024 from 95.127.68.34
ubuntu@ip-172-31-30-29:~$ |
```

4. Configuración del servidor ssh Linux

A continuación, se han modificado algunas configuraciones básicas y otras no, que son las siguientes:

- LoginGraceTime 2m

Se cambió a LoginGraceTime 1m

Razón. Reduce el tiempo que el servidor espera para iniciar sesión antes de desconectar, lo que puede ayudar a prevenir ataques de fuerza bruta.

- PermitRootLogin prohibit-password

Se cambió a PermitRootLogin no

Razón. Desactiva el inicio de sesión del usuario root directamente, lo que es más seguro. En su lugar, los usuarios deben conectarse con una cuenta normal y usar sudo para ejecutar comandos con privilegios.

- StrictModes yes

Se mantuvo en StrictModes yes

Razón. Este parámetro ya está habilitado de forma predeterminada y verifica los permisos y la propiedad de los archivos de clave pública del usuario. Es recomendable mantenerlo en yes para asegurar que las configuraciones de seguridad de los archivos sean correctas.

- MaxAuthTries 6

Se cambió a MaxAuthTries 3

Razón. Reduce el número de intentos de autenticación fallidos antes de que se bloquee la sesión. Esto ayuda a mitigar los ataques de fuerza bruta.

- MaxSessions 10

Se cambió a MaxSessions 2

Razón. Limitar el número de sesiones simultáneas por conexión. Esto reduce el riesgo de que un atacante tome control de múltiples sesiones.

- PubkeyAuthentication yes

Se mantuvo en PubkeyAuthentication yes

Razón. Este parámetro debería permanecer habilitado para usar la autenticación de clave pública, que es más segura que las contraseñas.

En el pantallazo tenemos los cambios (sin las almohadillas que son para explicar)

```
GNU nano 7.2                               /etc/ssh/sshd_config *
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

LoginGraceTime 1m                         # Reduce el tiempo de gracia para iniciar sesión#
PermitRootLogin no                         # Desactiva el inicio de sesión del usuario root
StrictModes yes                            # Mantiene las comprobaciones de permisos en los archivos de claves
MaxAuthTries 3                             # Número máximo de intentos de autenticación fallidos
MaxSessions 2                             # Número máximo de sesiones simultáneas por conexión
PubkeyAuthentication yes                     # Habilita la autenticación de clave pública

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile    .ssh/authorized_keys .ssh/authorized_keys2
```

Ahora vamos a configurar un alias para conectarnos frecuentemente sin poner todo el tocho del comando de ssh. Lo primero será crear un archivo config (tenemos que quitar la extensión .txt). Le asignaremos un nombre de host al gusto y pondremos los siguientes parámetros:

```
config.txt

Archivo   Editar   Ver

Host SergioGSSH
  ubuntu| ec2-34-229-138-145.compute-1.amazonaws.com
  User ubuntu
  Port 222
  IdentityFile C:\Users\sergi\Desktop\SergioG_P12_Server1.pem
```

Ahora ya podremos hacer el comando “ssh xxx” siendo xxx el nombre del host que hemos asignado.

```
PS C:\Users\sergi\.ssh> ssh SergioGSSH
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

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

System information as of Tue Oct 22 17:11:30 UTC 2024

System load:  0.0          Processes:           106
Usage of /:   23.5% of 6.71GB  Users logged in:    0
Memory usage: 20%          IPv4 address for enX0: 172.31.30.29
Swap usage:   0%          

Expanded Security Maintenance for Applications is not enabled.

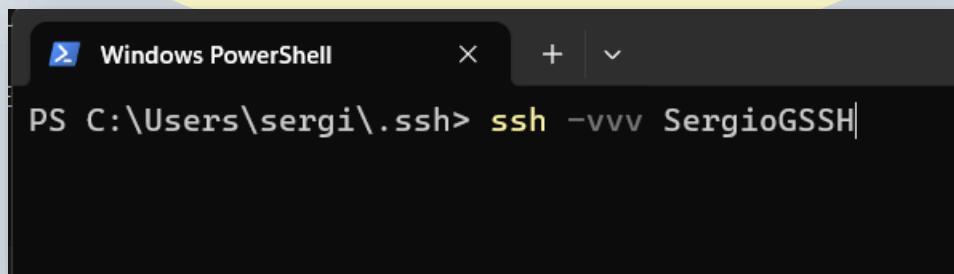
0 updates can be applied immediately.

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: Tue Oct 22 17:10:49 2024 from 95.127.68.34
ubuntu@ip-172-31-30-29:~$ |
```

Si nos llega a dar fallo, podemos poner el comando en pantalla, que puede solucionar que no encuentre el hostname.



5. Generar las claves con el comando keygen

En esta parte de la práctica, generaremos unas claves ssh-keygen, que nos darán un libre control de nuestro acceso con los archivos creados.

Para hacer esto, lo primero que debemos colocar es el comando keygen para que se creen.

```
sergiol@ip-172-31-30-29:/home/ubuntu$ cd ..
sergiol@ip-172-31-30-29:/home$ ls
sergiol sergio2 sergio3 ubuntu
sergiol@ip-172-31-30-29:/home$ cd sergiol
sergiol@ip-172-31-30-29:~$ ls
sergiol@ip-172-31-30-29:~$ ssh-keygen -b 4096 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sergiol/.ssh/id_rsa):
Created directory '/home/sergiol/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sergiol/.ssh/id_rsa
Your public key has been saved in /home/sergiol/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:9NYupT66/s3NnvePUQZ6tiUdNs3wnZ8YLNAvfx4nAlY sergiol@ip-172-31-30-29
The key's randomart image is:
+---[RSA 4096]---+
| .. . .
| ..E ++
| . o.o.==
| .oo.o+o=
| S.o.*.+.*
| . +.+.0.
| o ..=.o
| ..+ o =.
| .++o.o.*.=
+---[SHA256]---+
sergiol@ip-172-31-30-29:~$ |
```

Como el comando scp no me funcionaba, la forma en que habilité las claves para su funcionamiento es coger los archivos generados, mostrarlos y copiar su contenido.

```
.../root/.ssh/authorized_keys
sergiol@ip-172-31-30-29:~$ cd .ssh
sergiol@ip-172-31-30-29:~/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQACQDbGc8YGD3A0BFCDBiYpwGXqmJe3mD08QmP6Dbf4I9zjrOMiDLt9iBbsjiiTVZ927HLgWHE9spTlw6j
BA8HNxZGFdv08ICRu7sg97KckmeuSOS5j9i3lWAtEfFmu4hkngooG/ulrzEVHdajxGKc1S1n1v9HDME4Uezux/awjudevR8xxL8jaJoGYvd+eCSlq
qW4J6biNcYYwGuUCmfPjpBGGYBJXVFt9210vaUMAHUuNeOcikwBEPkDyeUC7CM17GwGuaCmAvhC1dKPCoBsb/Laiz1G0kBjEefvtBX67AiP5SQ2hnMUs
K+fezIMrzlmt6RmbHptZGratQ5Tg+E0BRXcjt0CCDJcyjImkzRY4V8w9SDRCd0Y2vc/LhRic8aaKgwCJMqX1RkU7a22RtkxwY0KMD5/EBg0xMgTR3jdYP
Su28QRV9q1kppc4jBBEbt5goRxVfczgoc/rXFUDdum4SDg53EguLP2C2VaDGQIRN0cZcq14FeZhAzvm0rkeK4f9z+qT9gr8r8YNV/DhiQj+wqyPRFfRea
wSFgcYdkdpqoy4igzxWjclLFIHRwT104jAhTeWl2CtmloN8R6FipWi2Ukszj043Ua/72ci6LiDf6NSXR+9IaCeEHdEndbeQe88ZPOR2dDNT6tCO+C80N
nIXr56F3XFaGppsoH4/Q== sergiol@ip-172-31-30-29
sergiol@ip-172-31-30-29:~/.ssh$ cat authorized_keys
sergiol@ip-172-31-30-29:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQACQDbGc8YGD3A0BFCDBiYpwGXqmJe3mD08QmP6Dbf4I9zjrOMiDLt9iBbsjiiTVZ927HLgWHE9spTlw6j
BA8HNxZGFdv08ICRu7sg97KckmeuSOS5j9i3lWAtEfFmu4hkngooG/ulrzEVHdajxGKc1S1n1v9HDME4Uezux/awjudevR8xxL8jaJoGYvd+eCSlq
qW4J6biNcYYwGuUCmfPjpBGGYBJXVFt9210vaUMAHUuNeOcikwBEPkDyeUC7CM17GwGuaCmAvhC1dKPCoBsb/Laiz1G0kBjEefvtBX67AiP5SQ2hnMUs
K+fezIMrzlmt6RmbHptZGratQ5Tg+E0BRXcjt0CCDJcyjImkzRY4V8w9SDRCd0Y2vc/LhRic8aaKgwCJMqX1RkU7a22RtkxwY0KMD5/EBg0xMgTR3jdYP
Su28QRV9q1kppc4jBBEbt5goRxVfczgoc/rXFUDdum4SDg53EguLP2C2VaDGQIRN0cZcq14FeZhAzvm0rkeK4f9z+qT9gr8r8YNV/DhiQj+wqyPRFfRea
wSFgcYdkdpqoy4igzxWjclLFIHRwT104jAhTeWl2CtmloN8R6FipWi2Ukszj043Ua/72ci6LiDf6NSXR+9IaCeEHdEndbeQe88ZPOR2dDNT6tCO+C80N
nIXr56F3XFaGppsoH4/Q== sergiol@ip-172-31-30-29
sergiol@ip-172-31-30-29:~/.ssh$ |
```

```
sergio1@ip-172-31-30-29:~/ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktbjEAAAABG5vbmUAQAAEbm9uZQAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAgEA2xnPGBg9wNARQgwYmKcBl6piXt5gzvEJ+jg23+CPc446zjIgy7FY
gW7I4ok1Wfduby4FhxPbKU5c0owQPbzV8xhXVaPCHEbs07BveynCpnrkjkuY/SN5VgLXhH
5rmuIZJ4KKBv7pa7mRLxw2o8ShpAtUp9b/R3TB0FHs7sf2sI7nXr0fMcS/CWiaBmL3fpxA
kpaqluCem4jXGMLhrlAphaYz/BhmASV1RbfotL2lDAB1LjXjgopMARKKSg2HlAuwjCOxs
BrmgpgFYQtXSjwqAbG/y2os9RkJASRHhb7QV+uwCKeUkNoZzFLCvn3syDK85ZrekZmx6bW
Rq2rUOU4PhNAUVwo7TgggyXMoyJpM0WOfMPUg0QnTmNr3Py4USHPGmioMAiTkl9UZF02t
tkbSscGNCjA+fxAYDqzIE0d43WD0rtvEEVfatZKaXOIwQRG7eYKEcVX3M4KHP61xVA3bpu
Eg40dxILiz9gtlWgxkCETdHGXXKpeBXmYQM75tK5HiuH/c/qk/YK/K/GDVfw4YkI/sksj0R
X0XmsEhYHL2HZHaaqMuKooM8Vo3CxSB0cEyNOIwIUxMC9grZpTp/EehYqVotlJLM490N1G
v+9nIui4g3+jUl0fvSGgnhB3RJ3W3kHvPGTzkdnQzU+rQjvgvNDZyF6+ehd1xWhqabKB+P
0AAAdQyAfCRcgHwkUAAAHC3NoLXjzYQAAAgEA2xnPGBg9wNARQgwYmKcBl6piXt5gzvEJ
j+g23+CPc446zjIgy7FYgW7I4ok1Wfduby4FhxPbKU5c0owQPbzV8xhXVaPCHEbs07Bvey
nCpnrkjkuY/SN5VgLXhH5rmuIZJ4KKBv7pa7mRLxw2o8ShpAtUp9b/R3TB0FHs7sf2sI7n
Xr0fMcS/CWiaBmL3fpxAkpaqluCem4jXGMLhrlAphaYz/BhmASV1RbfotL2lDAB1LjXjg
opMARKKSg2HlAuwjCOxsBrmgpgFYQtXSjwqAbG/y2os9RkJASRHhb7QV+uwCKeUkNoZzFL
Cvn3syDK85ZrekZmx6bWRq2rUOU4PhNAUVwo7TgggyXMoyJpM0WOfMPUg0QnTmNr3Py4U
SHPGmioMAiTkl9UZF02ttkbSscGNCjA+fxAYDqzIE0d43WD0rtvEEVfatZKaXOIwQRG7eY
KEcVX3M4KHP61xVA3bpuEg40dxILiz9gtlWgxkCETdHGXXKpeBXmYQM75tK5HiuH/c/qk/Y
K/K/GDVfw4YkI/sksj0RX0XmsEhYHL2HZHaaqMuKooM8Vo3CxSB0cEyNOIwIUxMC9grZpT
p/EehYqVotlJLM490N1Gv+9nIui4g3+jUl0fvSGgnhB3RJ3W3kHvPGTzkdnQzU+rQjvgvN
DZyF6+ehd1xWhqabKB+P0AAAADAQABAAACAC/zPEg+5+bmcIx0xr5D0HyniJtQCjpH9KqG
pNmJpM5impgNbHCP1D0as5YwocCEWHiufpavLmu+1T/b+n1D+k6T92c5vk1f62pFemot+4+a
```

Tanto la clave pública como la privada la copié y pégue a mi ordenador anfitrión para poder iniciar como mi usuario sin fallos.

Nombre	Fecha de modificación	Tipo	Tamaño
config	24/10/2024 18:50	Archivo	1 KB
id_rsa	24/10/2024 20:03	Archivo	4 KB
id_rsa	24/10/2024 20:01	Archivo PUB	1 KB
known_hosts	24/10/2024 19:04	Archivo	4 KB
known_hosts.old	22/10/2024 18:10	Archivo OLD	3 KB
SergioG_P12_Server1.pem	22/10/2024 17:50	Archivo PEM	2 KB

Ahora que tenemos los archivos, si utilizo la clave privada, podré acceder mediante uso de la contraseña (porque habilité inicio por contraseña en el sshd_config).

```
PS C:\Users\sergi> ssh -i C:\Users\sergi\.ssh\id_rsa -p 222 sergio1@98.81.175.88
Load key "C:\\\\Users\\\\sergi\\\\.ssh\\\\id_rsa": invalid format
sergio1@98.81.175.88's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

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

System information as of Thu Oct 24 18:03:59 UTC 2024

  System load:  0.0          Processes:           106
  Usage of /:   25.3% of 6.71GB  Users logged in:    0
  Memory usage: 21%
  Swap usage:   0%          IPv4 address for enX0: 172.31.30.29

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

sergio1@ip-172-31-30-29:~$ |
```

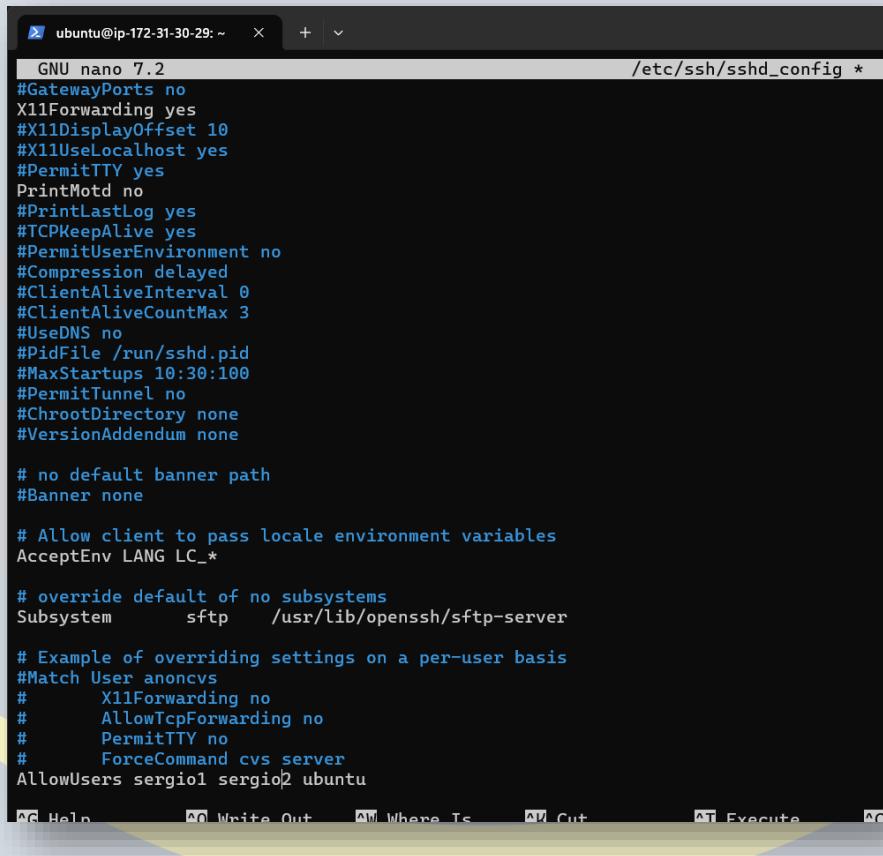
Al final también lo pude hacer de la forma que pide la práctica:

```
sergio1@ip-172-31-30-29:~$ scp -P 222 .ssh/id_rsa.pub sergio1@ec2-54-173-7-82.compute-1.amazonaws.com:.ssh/id_rsa.pub
The authenticity of host '[ec2-54-173-7-82.compute-1.amazonaws.com]:222 ([172.31.30.29]:222)' can't be established.
ED25519 key fingerprint is SHA256:FLU0+eI2zuDSQRFVnXnBW8JynDxtwKX8lg+e806DiU.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:2: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[ec2-54-173-7-82.compute-1.amazonaws.com]:222' (ED25519) to the list of known hosts.
scp: dest open ".ssh/id_rsa.pub": Permission denied
scp: failed to upload file .ssh/id_rsa.pub to .ssh/id_rsa.pub
sergio1@ip-172-31-30-29:~$ cd .ssh/
sergio1@ip-172-31-30-29:~/ssh$ ls -la
total 28
drwx----- 2 sergio1 sergio1 4096 Oct 25 07:04 .
drwxr-x--- 16 sergio1 sergio1 4096 Oct 25 07:01 ..
-rw----- 1 sergio1 sergio1 749 Oct 24 17:08 authorized_keys
-rw-rw-r-- 1 sergio1 sergio1 749 Oct 25 07:04 authorized_keys
-rw----- 1 sergio1 sergio1 3389 Oct 24 17:00 id_rsa
-r----- 1 sergio1 sergio1 749 Oct 24 17:00 id_rsa.pub
-rw-r--r-- 1 sergio1 sergio1 426 Oct 25 07:06 known_hosts
sergio1@ip-172-31-30-29:~/ssh$ chmod 600 id_rsa.pub
sergio1@ip-172-31-30-29:~/ssh$ ls -la
total 28
drwx----- 2 sergio1 sergio1 4096 Oct 25 07:04 .
drwxr-x--- 16 sergio1 sergio1 4096 Oct 25 07:01 ..
-rw----- 1 sergio1 sergio1 749 Oct 24 17:08 authorized_keys
-rw-rw-r-- 1 sergio1 sergio1 749 Oct 25 07:04 authorized_keys
-rw----- 1 sergio1 sergio1 3389 Oct 24 17:00 id_rsa
-r----- 1 sergio1 sergio1 749 Oct 24 17:00 id_rsa.pub
-rw-r--r-- 1 sergio1 sergio1 426 Oct 25 07:06 known_hosts
sergio1@ip-172-31-30-29:~/ssh$ cd ..
sergio1@ip-172-31-30-29:~$ scp -P 222 .ssh/id_rsa.pub sergio1@ec2-54-173-7-82.compute-1.amazonaws.com:.ssh/id_rsa.pub
id_rsa.pub
sergio1@ip-172-31-30-29:~$ |
```

6. Lista blanca y negra

La lista blanca se usa para permitir el inicio de sesión por ssh, mientras que la negra deniega. Realmente, si ponemos los usuarios permitidos en la blanca, ya sabemos quién tendrá acceso, ya que, si no están, pues no entran.

Para ello permitiremos el acceso a los usuarios 1, 2 y Ubuntu.



```
GNU nano 7.2 /etc/ssh/sshd_config *
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

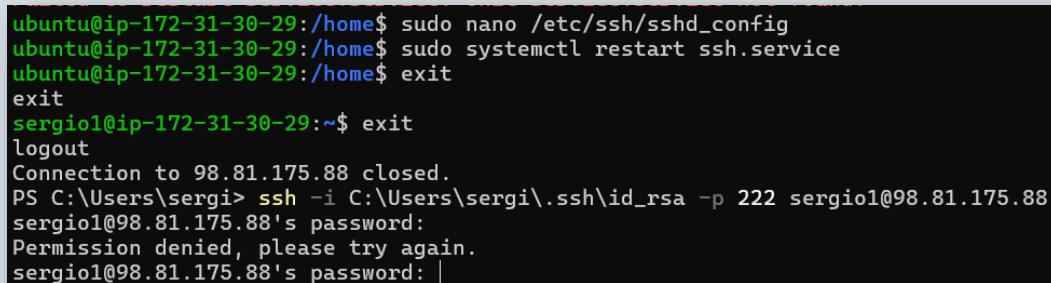
# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem      sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#   X11Forwarding no
#   AllowTcpForwarding no
#   PermitTTY no
#   ForceCommand cvs server
AllowUsers sergio1 sergio2 ubuntu
```

En el punto 5 de esta práctica ya estaba configurado el sshd_config para permitir a sergio1, así que, para ahorrar tiempo, pues le denegaré el permiso y comprobaremos que no puede acceder.



```
ubuntu@ip-172-31-30-29:/home$ sudo nano /etc/ssh/sshd_config
ubuntu@ip-172-31-30-29:/home$ sudo systemctl restart ssh.service
ubuntu@ip-172-31-30-29:/home$ exit
exit
sergio1@ip-172-31-30-29:~$ exit
logout
Connection to 98.81.175.88 closed.
PS C:\Users\sergi> ssh -i C:\Users\sergi\.ssh\id_rsa -p 222 sergio1@98.81.175.88
sergio1@98.81.175.88's password:
Permission denied, please try again.
sergio1@98.81.175.88's password: |
```

7. Conexión a servidor Linux sin usar claves criptográficas

Para conectararme sin usar clave criptográfica sólo tuve que poner el usuario y su IP, ya que tengo habilitado “PasswordAuthentication yes” en el sshd_config.

Podría deshabilitar “PubkeyAuthentication”, pero sería mucha movida si no tienes seguro el acceso sin clave criptográfica. Si hemos modificado el archivo de config, recordar hacer systemctl restart ssh.

Si todo funciona correctamente, deberíamos poder hacer el login con el siguiente comando:

```
C:\Users\sergi> ssh -p 222 sergio1@98.81.175.88
Load key "C:\Users\sergi\.ssh/id_rsa": invalid format
sergio1@98.81.175.88's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

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

System information as of Thu Oct 24 18:10:28 UTC 2024

System load:  0.0          Processes:           107
Usage of /:   25.3% of 6.71GB  Users logged in:      0
Memory usage: 20%          IPv4 address for enX0: 172.31.30.29
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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: Thu Oct 24 18:04:00 2024 from 95.127.69.49
sergio1@ip-172-31-30-29:~$ |
```

sergio1@ip-172-31-30-29:~\$ |
Last login: Thu Oct 24 18:04:00 2024 from 95.127.69.49
en.69.49.24.31.30.29:~\$ |
To check for new updates run: sudo apt update
The list of available updates is more than a week old.

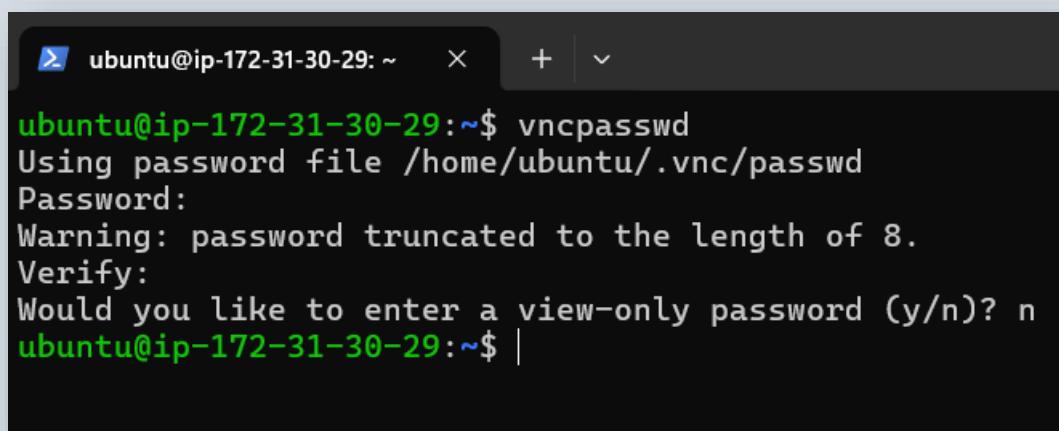
8. Escritorio remoto

En la instancia del servidor Ubuntu instalaremos un escritorio Xfce con los siguientes comandos:

```
ubuntu@ip-172-31-30-29:~$ sudo apt install xfce4
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
accountsservice accountsservice-ubuntu-schemas acl activity-log-manager adwaita-icon-theme alsamixer-conf apg aspell aspell-en at-spi2-common
bamfdaemon bluez-obexd bubblewrap cheese-common colord colord-data cpp cpp-13 cpp-13-x86-64 linux-gnu cpp-x86-64-linux-gnu cracklib-runtime cups cups-bi-
cups-daemon cups-filters cups-filters-core-drivers cups-ipp-utils cups-pk-helper cups-ppdc cups-server-common dconf-dconf-service
dictionaries-common dns-root-data dnsmasq-base docbook-xml elementary-xfce-icon-theme emacsen-common enchant-2 evolution-data-server evolution-data-server-common
fonts-dejavu-core fonts-dejavu-mono fonts-droid-fallback fonts-noto-mono fonts-quicksand fonts-ubuntu fonts-urw-base35 gcc-13-base gcr gcr4 geocode-glib-comm
girl-2-dbusmenu libglib-0.4 girl-2-freedesktop girl-2-gdkpixbuf-2.0 girl-1.2-gtk-3.0 girl-2-handy-1 girl-2-harfuzz-0.0 girl-2ibus-1.0 girl-2-notify-0.7 girl-1.2-pi
gkbd-capplet glib-networking glib-networking-services gnome-bluetooth gnome-bluetooth-3-common gnome-blueooth-sendo gnome-control-center
gnome-keyring-pkcs11 gnome-menu gnome-power-manager gnome-screensaver gnome-session-bin gnome-session-common gnome-settings-daemon-common gnome-startup-applications
gobjxbird-gtk-theme gsettings-desktop-schemas gsettings-ubuntu-schemas gstreamer1.0-clutter-0.0 gstreamer1.0-gstbase gstreamer1.0-plugins-base gstreamer1.0-audio
gstreamer1.0-audio-xfce gstreamer1.0-gstbase gstreamer1.0-gstbase-xfce gstreamer1.0-gstbase-xfce-0.0.965 gstreamer1.0-plugins-base ibus ibus-indicator
indicator-applet indicator-application indicator-applets indicator-bluetooth indicator-keyboard indicator-messages indicator-sounds indicator-timezone indicator-datetime
indicator-sound intel-media-video-driver ipp-usa jayatana libai1 libabsl20220623t64 libaccounts-glib0 libaccounts-service0 libadwaita-1.0 libaudio libasound2-data
libasyncts9 libatk-bridge2.0-0t64 libatk1.0-0t64 libatkmm-1.6-1v5 libatomic1 libatspi2.0-0t64 libavahi-client libavahi-common-data libavahi-common2 libavahi-
libavutil58 libavatana-appindicator3-1 libavatana-ido3-0.4-0 libavatana-indicator3-7 libbamf3-2t64 libbluetooth3 libcacaf9 libcairo-gobject2 libcairo-script-in
libcamel-1.2-6ut64 libcanberra-gtk3-0t64 libcanberra-pulse libcdio-cdda2t64 libcdio-paranoia2t64 libcdio19t64 libcdpa1 libclutter-1.0-0 libclutter-1.0-common libclutter-gst-3.0-0 libclutter-gtk-1.0-0 libcodec2-1.2 libcogl-common libcogl-pango29 libcogl-path20 libegl20 libglc0
libglcutter-1.0-0 libglcutter-gst-3.0-0 libglcutter-gtk3-0-0 libglcutter-gtk3-3 libglconf1 libde265-0 libdee-1 libdrm-nouveau2 libdrm-radeon1 libdv4t64 libebackend-1.2-11t64 libebook-1.2-21t64 libebook-contacts-1.2-4t64 libecal-2.0-3 libedata-book-1.2-27t64 libedata-c
libedataserver-1.2-4t64 libegl-mesa0 libegl1 libenchant-2-2 libepoxy0 libesif12 libexo-2-0 libexo-common libfcitx-configuration libfcitx-gclient libfcitx-utils8
libfontenc1 libgail-common libgail18t64 libgarcon-1 libgarcon-common libgarcon-gtk3-1-0 libgbm1 libgck-1-0 libgck-2-2 libgcr-4-4 libgcr-base-3-1 libgcr-ui-
libgdg-pixbuf2-0-0 libgdg-pixbuf2.0-bin libgdg-pixbuf2.0-common libgee-0.8-2 libgeocode-glib-2-0 libgeonames-common libgeonames0 libglib1 libglib1-amber-dr lib
libglibmm-2.4-1t64 libglu1-mesa libglvnd0 libglx-mesa0 libgx0 libgname-bluetooth-3.0-13 libgname-desktop-3-20t64 libgname-menu-3-0 libgname-panel3 libgnomek
libgoa-1.0-common libgomp1 libgphoto2-6t64 libgphoto2-1l0n-x libgphoto2-port12t64 libgraphene-1.0-0 libgraphite-2-3 libgs-common libgs10 libgs10-common libgsml1
libgstreamer-plugins-base1.0-0 libgstreamer-plugins-good1.0-0 libgtk-3-0t64 libgtk-3-bin libgtk-4-1 libgtk-4-bin libgtk-4-common libgtk-4-med
libgtk-2.0-common libgtkmm-3.0-1t64 libgttop-2-0 libgttop2-common libgweather-4-0t64 libgweather-4-common libhandy-1-0 libharfbuzz-gobject libharfbuzz-icu1
libheif-plugin-aomenc libheif-plugin-libde265 libheif1 libhusbnr1 libhusbnr1 libhusbnr1 libibus0 libibusmenu-gtk3-1 libude265-0 libdee-1 libied
libimobiledevice6 libindicator3-7 libinput-bin libinput10 libjack-jackd2-0 libjavasciptcoregtk-4.1-0 libjbig0 libjbig2dec0 libjpeg-turbo8 libjpeg8
liblcr4 liblightdm-gobject-1-0 liblcr17t64 liblouis-data liblouis2 liblouisutdml-data liblouisutdml9t64 libltdl7 libmanette-0.2-0 libmes
libmsgraph-0.1 libmtdev1t64 libmtp-common libmtp-runtime libmtp9t64 libnautilus-extension4 libndp0 libnfs14 libnma0 libnma-common libnotify-bin libnot
libopus0 librcore-0.4-0t64 libpan-gnome-keyring libpango-1.0-0 libpangoft2-1.0-0 libpangocairo-1.4-1v5 libpangoft2-1.0-0 libpaper-utils libpap
libpinyin-wire-0.3-0t64 libpinyin-wire-0.3-common libpinyinman-1.0 libplist-2.0-0 libpoppler-cognit64 libpoppler-clip8t64 libpoppler134 libpoppler2 libpop
libproto
```

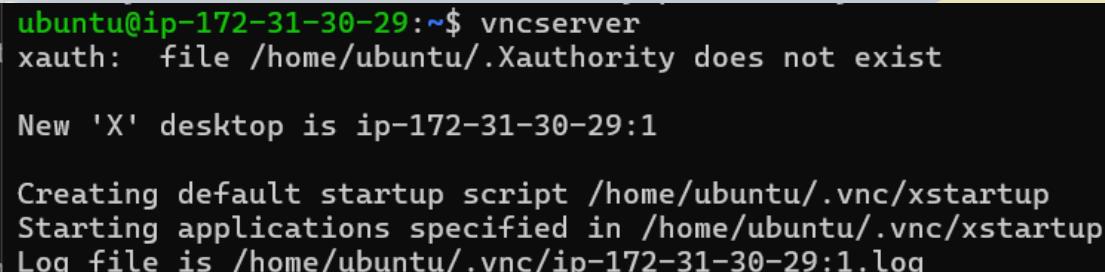
```
ubuntu@ip-172-31-30-29:~$ sudo apt-get install xfce4 xfce4-goodies tightvncserver
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
xfce4 is already the newest version (4.18).
The following additional packages will be installed:
7zip bzip2 libauthen-sasl-perl libburn4t64 libclone-perl libdata-dump-perl libencode-locale-perl
libgspell-1-2 libgspell-1-common libgtk-layer-shell0 libgtksourceview-4-0 libgtksourceview-4-comm
libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl libhttp-negotiate
liblwp-mediatypes-perl liblwp-protocol-https-perl libmailtools-perl libmousepad0 libnet-dbus-perl
libtimedate-perl libtry-tiny-perl libwww-perl libwww-robotrules-perl libxml1-protocol-perl libxml-
perl-openssl-defaults ristretto thunar-archive-plugin thunar-media-tags-plugin tightvncpasswd unz
xfce4-cpugraph-plugin xfce4-dict xfce4-diskperf-plugin xfce4-fsguard-plugin xfce4-gemmon-plugin x
xfce4-power-manager-plugins xfce4-screenshooter xfce4-sensors-plugin xfce4-smartbookmark-plugin x
xfce4-wavelan-plugin xfce4-weather-plugin xfce4-whiskermenu-plugin xfce4-xkb-plugin
Suggested packages:
7zip-standalone 7zip-rar bzip2-doc libdigest-hmac-perl libgssapi-perl libio-compress-brotli-perl
xml-twig-tools fancontrol read-edid i2c-tools debhelper heif-gdk-pixbuf libavif-gdk-pixbuf libjxl
ncompress pbzip2 pigz plzip rar unar gigolo parole xfce4-indicator-plugin xfce4-mpc-plugin xfce4-
The following NEW packages will be installed:
7zip bzip2 libauthen-sasl-perl libburn4t64 libclone-perl libdata-dump-perl libencode-locale-perl
libgspell-1-2 libgspell-1-common libgtk-layer-shell0 libgtksourceview-4-0 libgtksourceview-4-comm
libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl libhttp-negotiate
liblwp-mediatypes-perl liblwp-protocol-https-perl libmailtools-perl libmousepad0 libnet-dbus-perl
libtimedate-perl libtry-tiny-perl libwww-perl libwww-robotrules-perl libxml1-protocol-perl libxml-
perl-openssl-defaults ristretto thunar-archive-plugin thunar-media-tags-plugin tightvncpasswd tig
xfce4-cpufreq-plugin xfce4-cpugraph-plugin xfce4-dict xfce4-diskperf-plugin xfce4-fsguard-plugin
xfce4-power-manager xfce4-power-manager-data xfce4-power-manager-plugins xfce4-screenshooter xfce
xfce4-timer-plugin xfce4-verve-plugin xfce4-wavelan-plugin xfce4-weather-plugin xfce4-whiskermenu
0 upgraded, 93 newly installed, 0 to remove and 0 not upgraded.
Need to get 14.4 MB of archives.
After this operation, 58.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] |
```

Una vez instalado, ejecutamos el comando vncpasswd para establecer la contraseña de acceso.



```
ubuntu@ip-172-31-30-29:~$ vncpasswd
Using password file /home/ubuntu/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
ubuntu@ip-172-31-30-29:~$ |
```

Para configurar el servidor de VNC, ejecutamos el comando vncserver para la creación de archivos de configuración por defecto. Se creará el fichero `~/.vnc/xstartup` que contiene los comandos de conexión y se lanzará una instancia predeterminada de servidor en el puerto 5901.



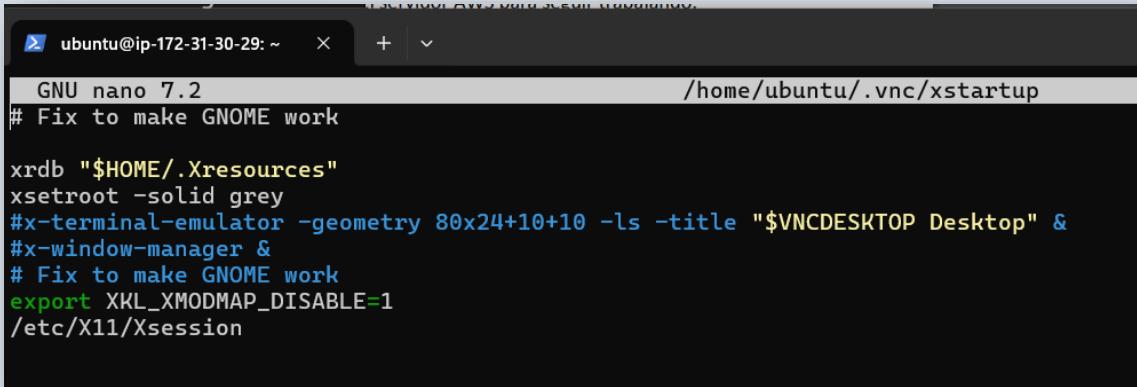
```
ubuntu@ip-172-31-30-29:~$ vncserver
xauth:  file /home/ubuntu/.Xauthority does not exist

New 'X' desktop is ip-172-31-30-29:1

Creating default startup script /home/ubuntu/.vnc/xstartup
Starting applications specified in /home/ubuntu/.vnc/xstartup
Log file is /home/ubuntu/.vnc/ip-172-31-30-29:1.log
```

Este puerto se llama un puerto de visualización, y se le conoce por VNC como :1. VNC puede lanzar varias instancias en otros puertos de visualización, como :2, :3, etc.. Cuando se trabaja con servidores VNC, Recuerda :X es un puerto de visualización que se refiere a 5900+X. Nosotros usamos la instancia del servidor VNC que se ejecuta en el puerto 5901.

Abrimos el script `~/.vnc/xstartup` y vemos la configuración: `nano ~/.vnc/xstartup`



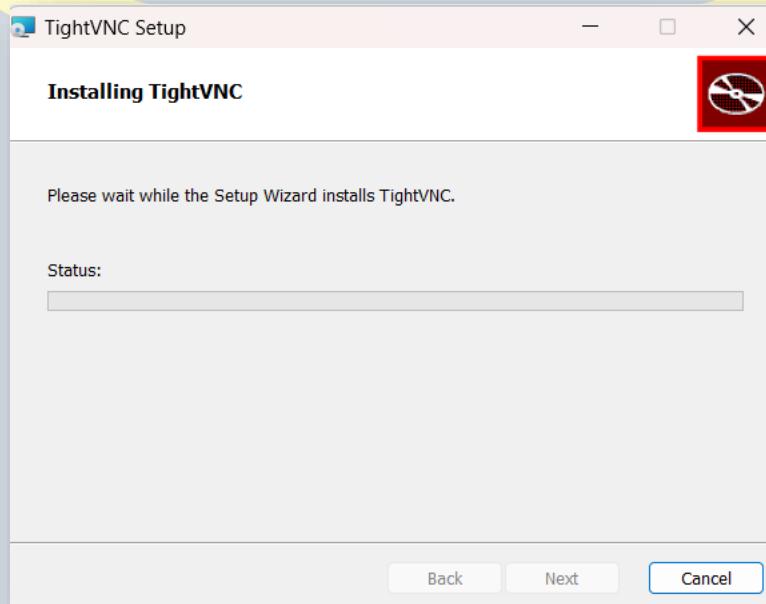
```
ubuntu@ip-172-31-30-29: ~      + | -      /home/ubuntu/.vnc/xstartup
GNU nano 7.2
# Fix to make GNOME work

xrdb "$HOME/.Xresources"
xsetroot -solid grey
#x-terminal-emulator -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
#x-window-manager &
# Fix to make GNOME work
export XKL_XMODMAP_DISABLE=1
/etc/X11/Xsession
```

Para asegurarse de que el servidor VNC será capaz de utilizar correctamente este nuevo archivo de arranque, vamos a necesitar conceder privilegios ejecutables.

```
ubuntu@ip-172-31-30-29:~$ nano ~/.vnc/xstartup
ubuntu@ip-172-31-30-29:~$ sudo chmod +x ~/.vnc/xstartup
ubuntu@ip-172-31-30-29:~$ |
```

Ya tenemos lista la instalación, ahora tendremos que instalar un cliente VNC, en mi caso TightVNC.



Importante antes abrir el puerto 5901 en el grupo de seguridad de la instancia del servidor, ya que, sin el puerto, pues no accederá.

The screenshot shows a web-based interface for managing network security rules. At the top, it says "Editar reglas de entrada" and "Reglas de entrada". Below this is a table with columns: ID de la regla del grupo de seguridad, Tipo, Protocolo, Intervalo de puertos, Origen, Descripción: opcional, and Eliminar. There are six existing rules and one new row being edited at the bottom:

ID de la regla del grupo de seguridad	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional	Eliminar
sgr-0c7aa636550b2591ed	HTTPS	TCP	443	Personalizada		<input type="button" value="Eliminar"/>
sgr-0e039a2fab9151bf	SSH	TCP	22	Personalizada		<input type="button" value="Eliminar"/>
sgr-0e680f6be2e9dbecf	HTTP	TCP	80	Personalizada		<input type="button" value="Eliminar"/>
sgr-04dd3e90cca1eb433	TCP personalizado	TCP	222	Personalizada	SSH	<input type="button" value="Eliminar"/>
-	TCP personalizado	TCP	5901	Anywhere-IPv4	VNC	<input type="button" value="Eliminar"/>

At the bottom left is a button labeled "Agregar regla".

Si todo va bien podremos hacer el login.

```

sergio1@ip-172-31-30-29: ~
Building dependency tree... Done
Reading state information... Done
tightvncserver is already the newest version (1:1.3.10-8).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
sergio1@ip-172-31-30-29:~$ nano ~/.vnc/xstartup
sergio1@ip-172-31-30-29:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
    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 noprefixroute
        valid_lft forever preferred_lft forever
2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state
    link/ether 00:0c:29:1b:31:25 brd ff:ff:ff:ff:ff:ff
    inet 172.31.31.255 brd 172.31.31.255 scope global dynamic
        valid_lft 2755sec
        inet6 fe80::20c:29ff:fe1b:3125/64 scope link
            valid_lft forever
            preferred_lft forever
sergio1@ip-172-31-30-29:~$ vnc Authentication
Connected to: 98.81.175.88:5901
Password: *****
OK Cancel
sergio1@ip-172-31-30-29:~$ New 'X' desktop is ip-172-31-30-29:1
Starting applications specified in /home/sergio1/.vnc/xstartup
Log file is /home/sergio1/.vnc/ip-172-31-30-29:1.log

sergio1@ip-172-31-30-29:~$ vncserver -kill :1
Killing Xtightvnc process ID 2422
sergio1@ip-172-31-30-29:~$ vncserver -kill :2
Killing Xtightvnc process ID 2101
sergio1@ip-172-31-30-29:~$ vncserver -kill :3
Killing Xtightvnc process ID 2644
sergio1@ip-172-31-30-29:~$ vncserver

New 'X' desktop is ip-172-31-30-29:1
Starting applications specified in /home/sergio1/.vnc/xstartup
Log file is /home/sergio1/.vnc/ip-172-31-30-29:1.log

sergio1@ip-172-31-30-29:~$
```

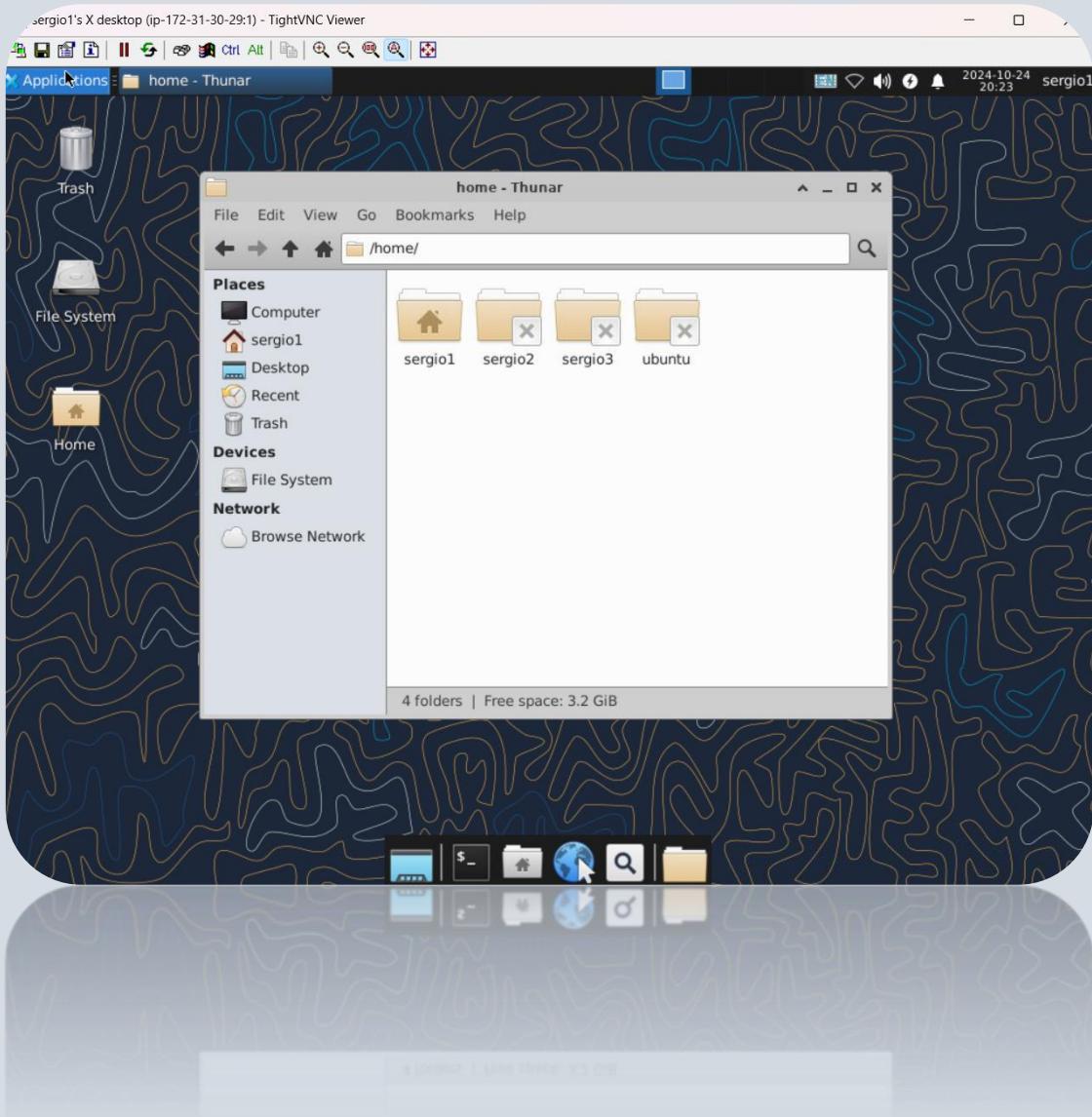
Como me sale la pantalla gris al conectarme, debemos retocar con el siguiente comando para que startxfce4 se encuentre en modo automático, tal y como muestra la siguiente imagen.

```
sergio1@ip-172-31-30-29:~/vnc$ sudo update-alternatives --config x-session-manager
There are 3 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).

Selection    Path          Priority   Status
-----      -----
0            /usr/bin/startxfce4    50        auto mode
1            /usr/bin/gnome-session  50        manual mode
* 2           /usr/bin/startxfce4    50        manual mode
3            /usr/bin/xfce4-session  40        manual mode

Press <enter> to keep the current choice[*], or type selection number: 2
sergio1@ip-172-31-30-29:~/vnc$ |
```

Cuando hagamos eso, faremos un sudo reboot y ya podremos acceder de forma correcta.



9. Crear un túnel ssh para acceso remoto a servicios

Ahora vamos a configurar un túnel SSH para acceder a un servicio en la instancia que normalmente no está disponible públicamente. Para hacer esto, debemos seguir una serie de pasos:

- Primer paso: Instalar apache en la instancia con su reseteo.

```
Last login: Thu Oct 24 20:22:12 2024 from 217.61.224.242
sergio1@ip-172-31-30-29:~$ sudo apt install apache2
[sudo] password for sergio1:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
  liblua5.4-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
  liblua5.4-0
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 2066 kB of archives.
After this operation, 8026 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

```
No VM guests are running outdated hypervisor (QEMU) binaries on this host.
sergio1@ip-172-31-30-29:~$ sudo systemctl start apache2
sergio1@ip-172-31-30-29:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
sergio1@ip-172-31-30-29:~$
```

- Segundo paso: Crear el túnel SSH: Desde la máquina local, crea un túnel SSH que redirija un puerto local al puerto 80 de la instancia EC2 (donde Apache está escuchando)

```
PS C:\Users\sergi1.ssh> ssh -i \Sergio1\Amazonaws.pem -L 8088:localhost:80 sergio1@ec2-54-173-7-82.compute-1.amazonaws.com -p 222
The authenticity of host '(ec2-54-173-7-82.compute-1.amazonaws.com):222 ([54.173.7.82]:222)' can't be established.
ED25519 key fingerprint is SHA256:FL4Q+H2zuDSQFvXnBw83ynDxtwXlg+e80G0jTU.
This host key is known by the following other names/addresses:
  C:\Users\sergi1\.ssh\known_hosts:11: ec2-34-229-138-145.compute-1.amazonaws.com
  C:\Users\sergi1\.ssh\known_hosts:14: [ec2-98-81-175-88.compute-1.amazonaws.com]:222
  C:\Users\sergi1\.ssh\known_hosts:15: [98.81.175.88]:222
  C:\Users\sergi1\.ssh\known_hosts:16: [18.208.211.177]:222
  C:\Users\sergi1\.ssh\known_hosts:17: [18.208.211.177]:222
Are you sure you want to connect (yes/no)? yes
Warning: Permanently added '[ec2-54-173-7-82.compute-1.amazonaws.com]:222' (ED25519) to the list of known hosts.
sergio1@ec2-54-173-7-82.compute-1.amazonaws.com's password:
Welcome to Ubuntu 24.04.1 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 Fri Oct 25 06:40:41 UTC 2024

System load: 0.67 Processes: 147
Usage of /: 52.7% of 6.71GB Users logged in: 0
Memory usage: 35% IPv4 address for enx0: 172.31.38.29
Swap usage: 0%

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

  https://ubuntu.com/pro

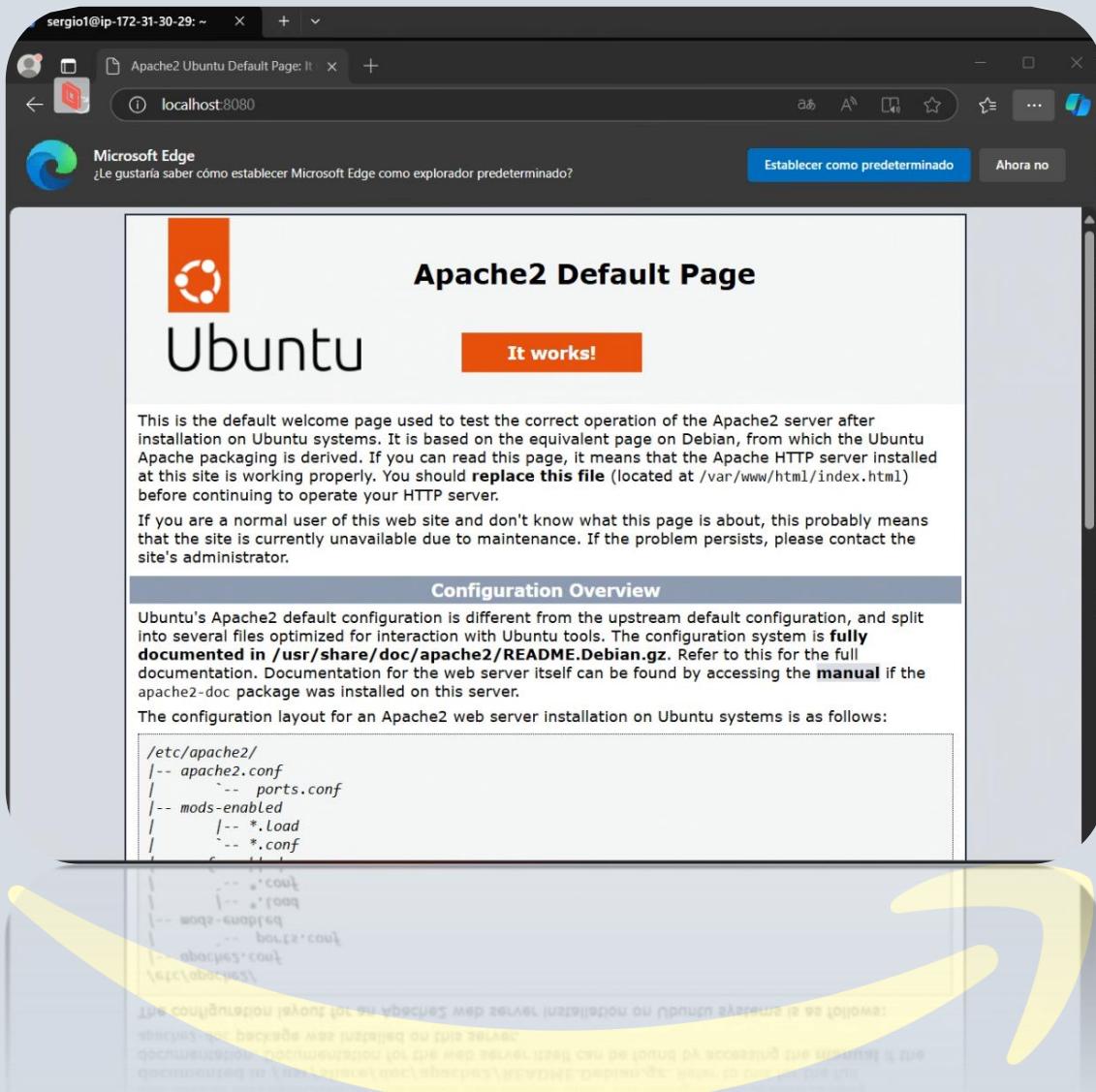
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Fri Oct 25 06:35:11 2024 from 217.61.224.242
sergio1@ip-172-31-30-29:~$
```

- Paso tres: Si todo va bien, si ponemos en nuestro PC local “localhost:8080” y nos debería salir el servidor de Apache correctamente instalado.



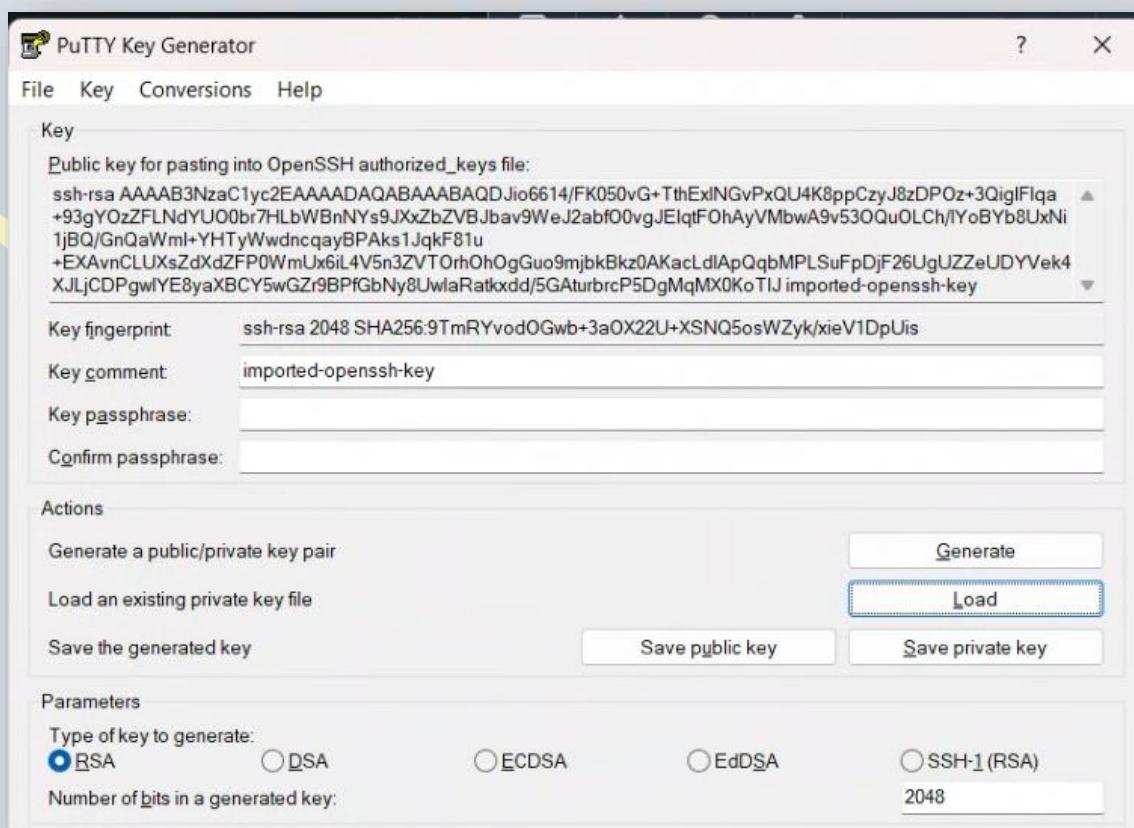
10. Tunel con Putty a servidor Web anterior

En este apartado emplearemos el cliente SSH PuTTY para crear el tunnel, pero podeis hacerlo con otro cliente diferente que tenga la opción de poder configurar túneles SSH.

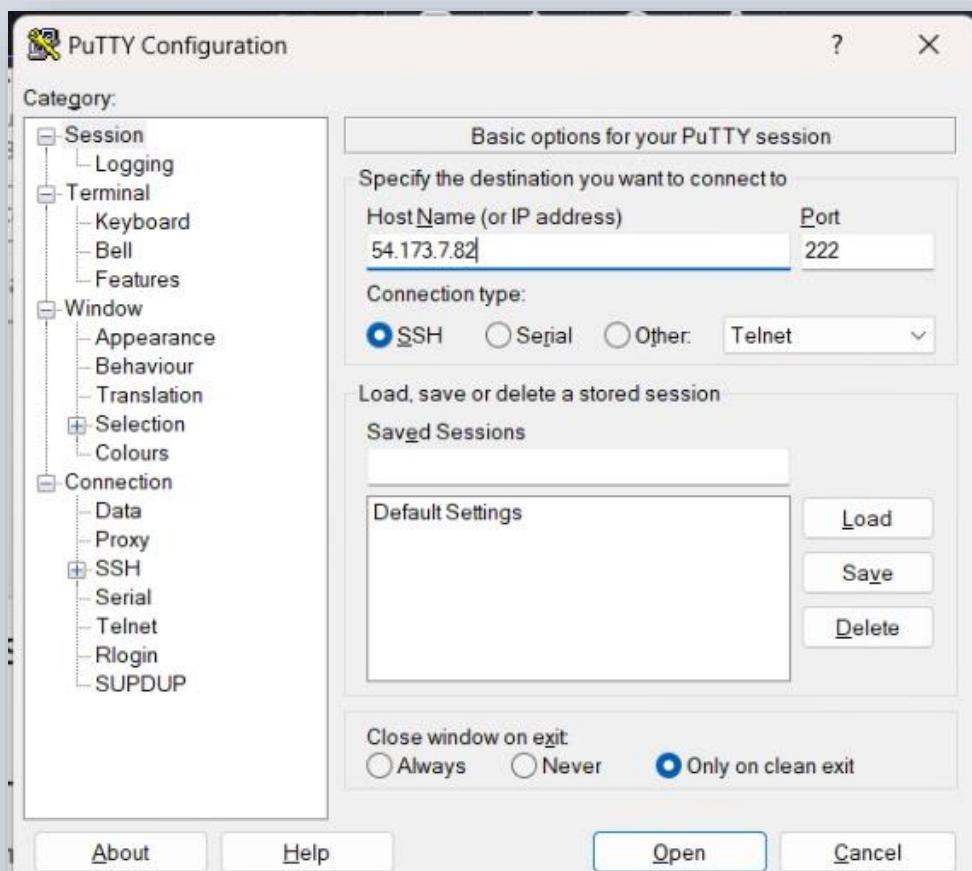
Vamos a configurar un túnel SSH local con PuTTY para redirigir una aplicación web que corre en un puerto específico del servidor remoto Ubuntu a nuestra máquina local Windows. El servicio al que queremos acceder es el servidor Web anterior.

El túnel se configura para conectarse a la IP del servidor por el puerto 22, una vez establecida la conexión al servidor SSH el cliente se conectará por Escritorio remoto a sí mismo (127.0.0.1 o localhost) por el puerto configurado en el túnel SSH, ese puerto redirigirá la conexión al servidor SSH que a su vez redirigirá a la IP interna del servidor que aceptará la conexión de Escritorio remoto.

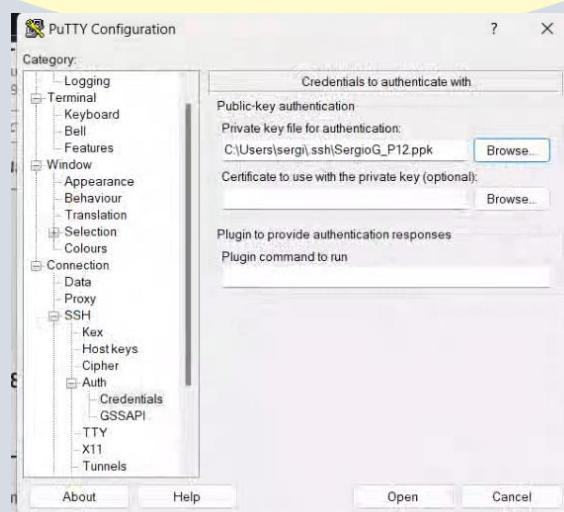
Para empezar la configuración, debemos ir al PuTTygen y cambiar la clave .pem a .ppk.



Una vez configurado, abriremos PuTTY, configurando la IP pública y el puerto por el que entramos.

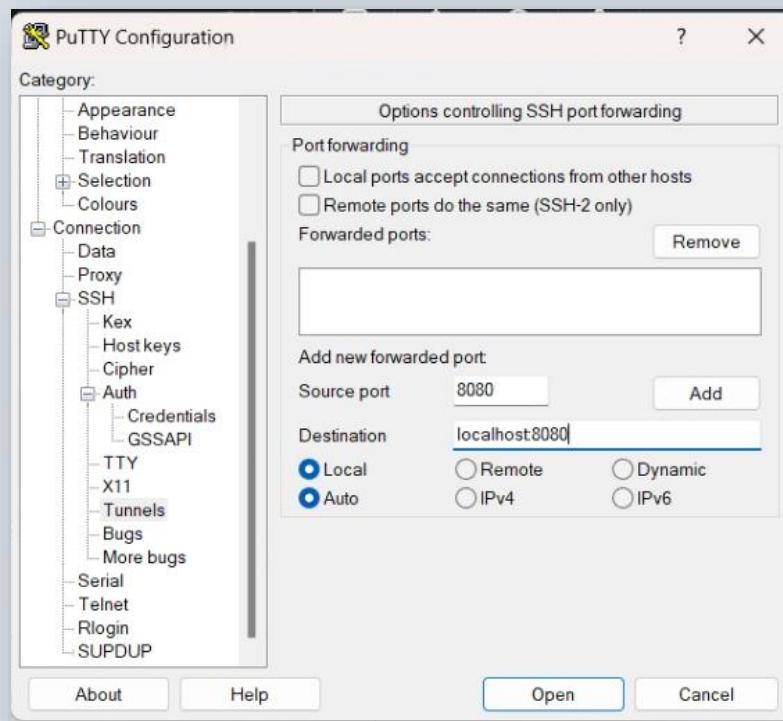


En las credenciales, meteremos el .ppk con la clave privada que acabamos de generar.

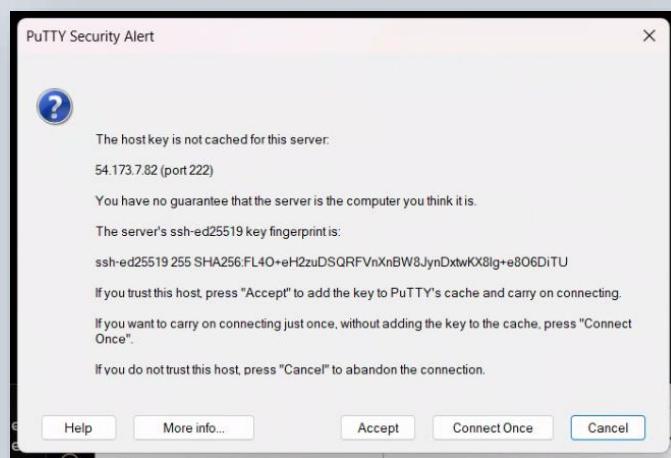


Para definir el túnel necesitas indicar el puerto origen "Source port", que es el puerto en el que el cliente simulará la aplicación no-segura y el puerto en el que la aplicación nosegura escucha realmente separado por dos puntos de la dirección IP del servidor.

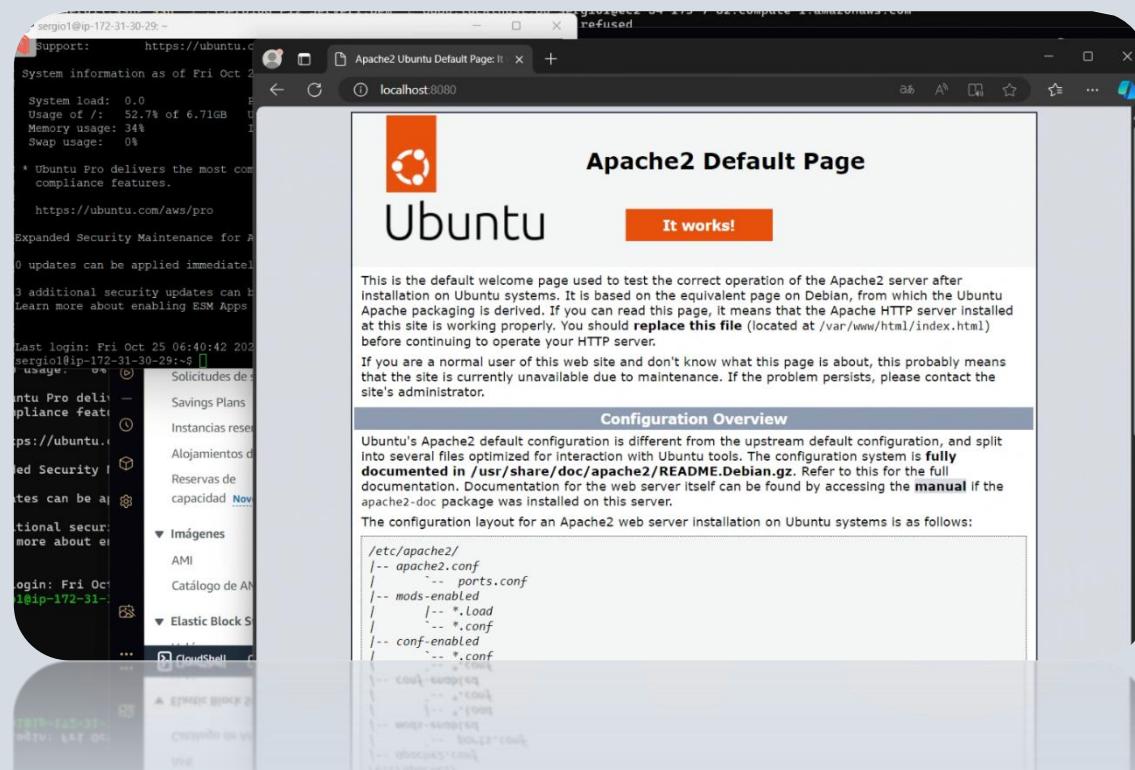
Sabiendo esto, iremos al menú de túneles e insertaremos lo siguiente, sin olvidar darle a add



Ahora podremos darle a “open” y nos podremos conectar.



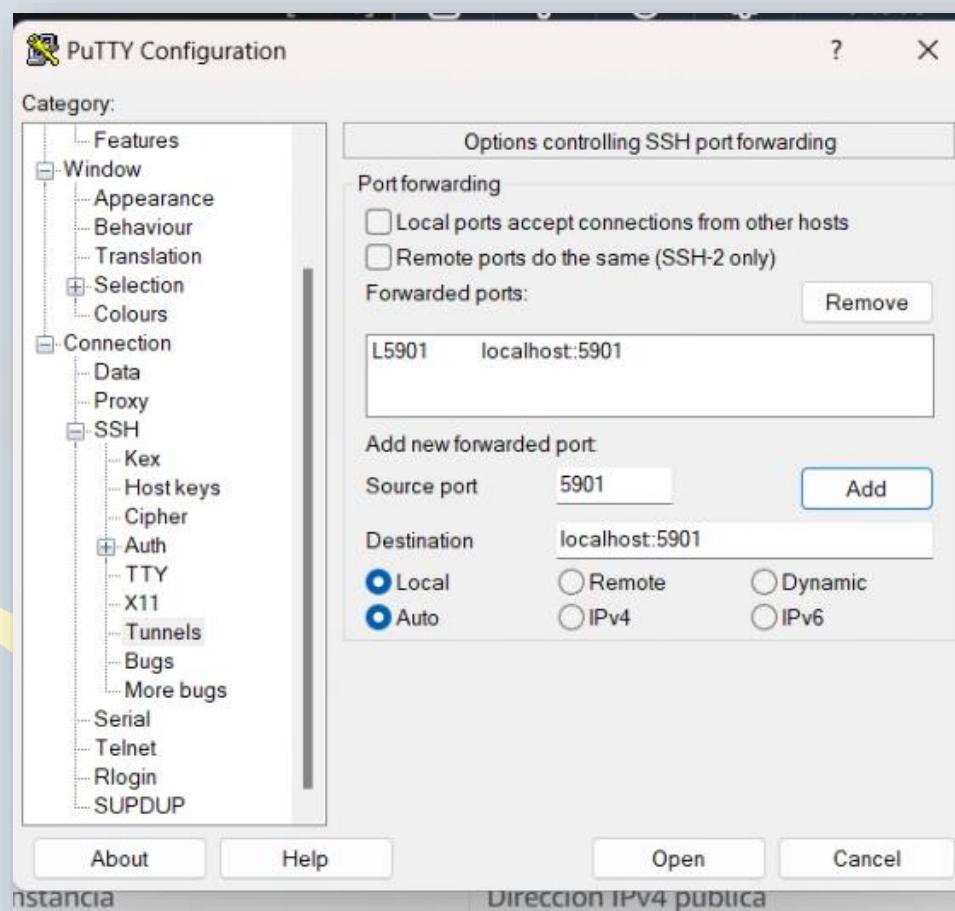
Una vez conectado al servidor, abrimos un navegador web en el equipo local y navegamos a <http://localhost:8080>. La página debería cargar como si estuviera accediendo directamente al servidor remoto, aunque el tráfico está siendo redirigido a través del túnel SSH.



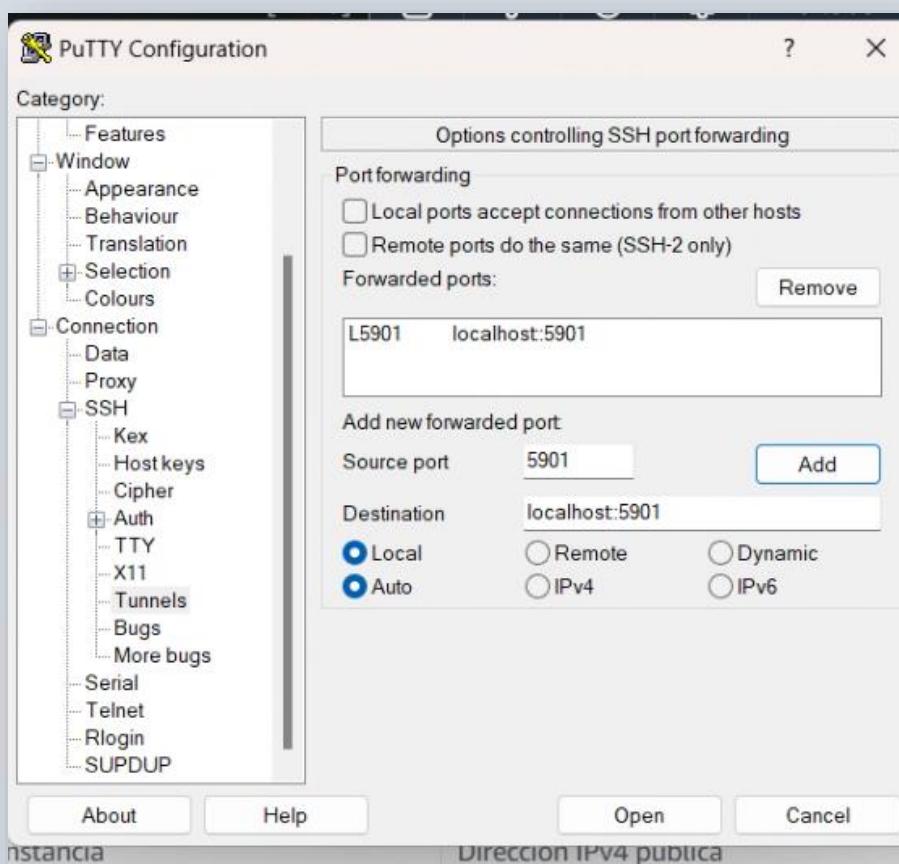
11. Tunel con Putty para conectarse a VNC

El objetivo de la práctica es Configurar un túnel SSH local con PuTTY para acceder al escritorio remoto del servidor Ubuntu en AWS usando VNC. Se usará un túnel SSH para redirigir el puerto de VNC del servidor al equipo local Windows. Para conseguirlo debemos seguir una serie de pasos:

- Abre PuTTY y coloca la IP pública del servidor en el campo "Host Name"



- Volvemos al menú de túneles e ingresamos 590. En Destination, ingresa localhost:5901 y le damos a add.



- Cargamos la clave privada y ya podremos darle a open.

A terminal window titled 'sergio1@ip-172-31-30-29: ~' displays system information. It includes details like system load (0.0), memory usage (58%), swap usage (0%), and network information (IPv4 address 172.31.30.29). The window also shows a message about Ubuntu Pro and ESM Apps, and ends with a 'Last login' timestamp.

```
sergio1@ip-172-31-30-29: ~
* Support: https://ubuntu.com/pro
System information as of Fri Oct 25 07:15:55 UTC 2024

System load: 0.0          Processes: 195
Usage of /: 52.7% of 6.71GB  Users logged in: 1
Memory usage: 58%          IPv4 address for enX0: 172.31.30.29
Swap usage: 0%

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

https://ubuntu.com/aws/pro

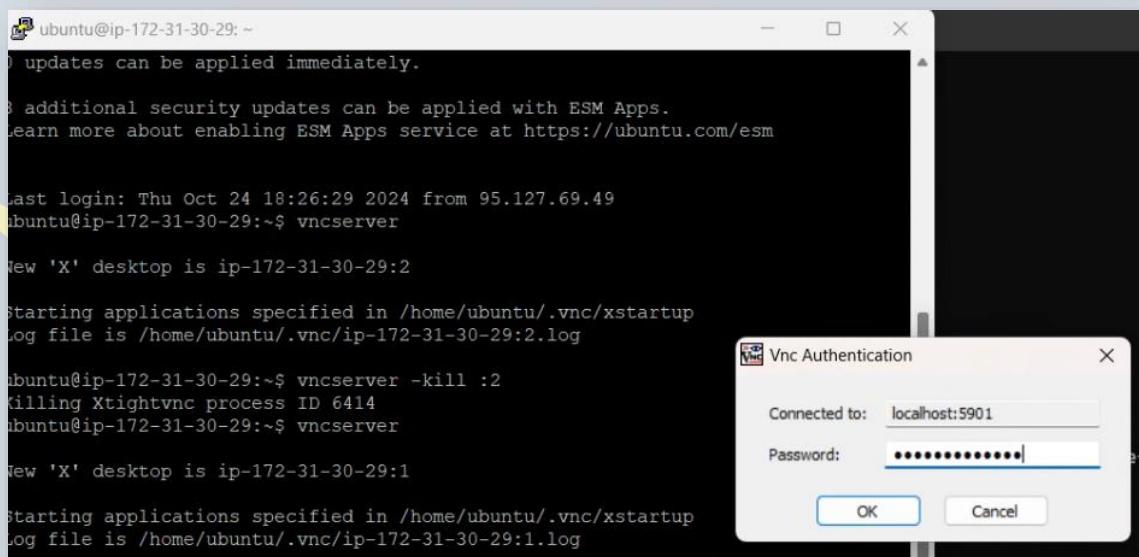
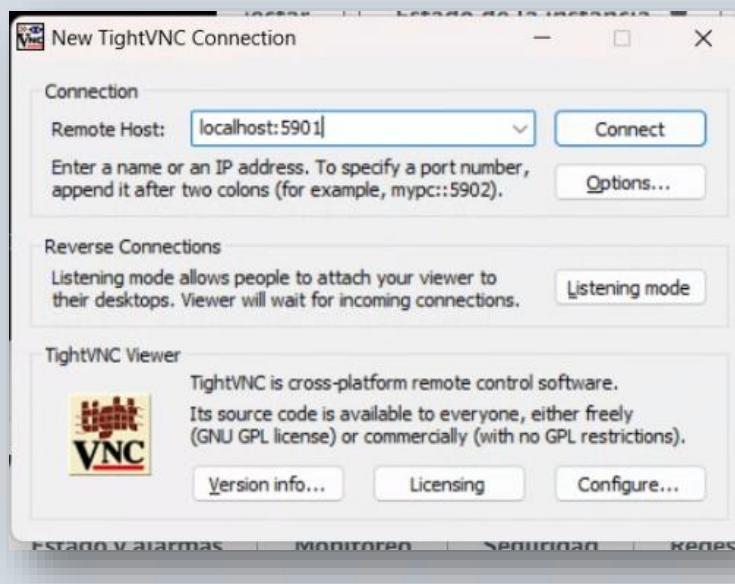
Expanded Security Maintenance for Applications is not enabled.

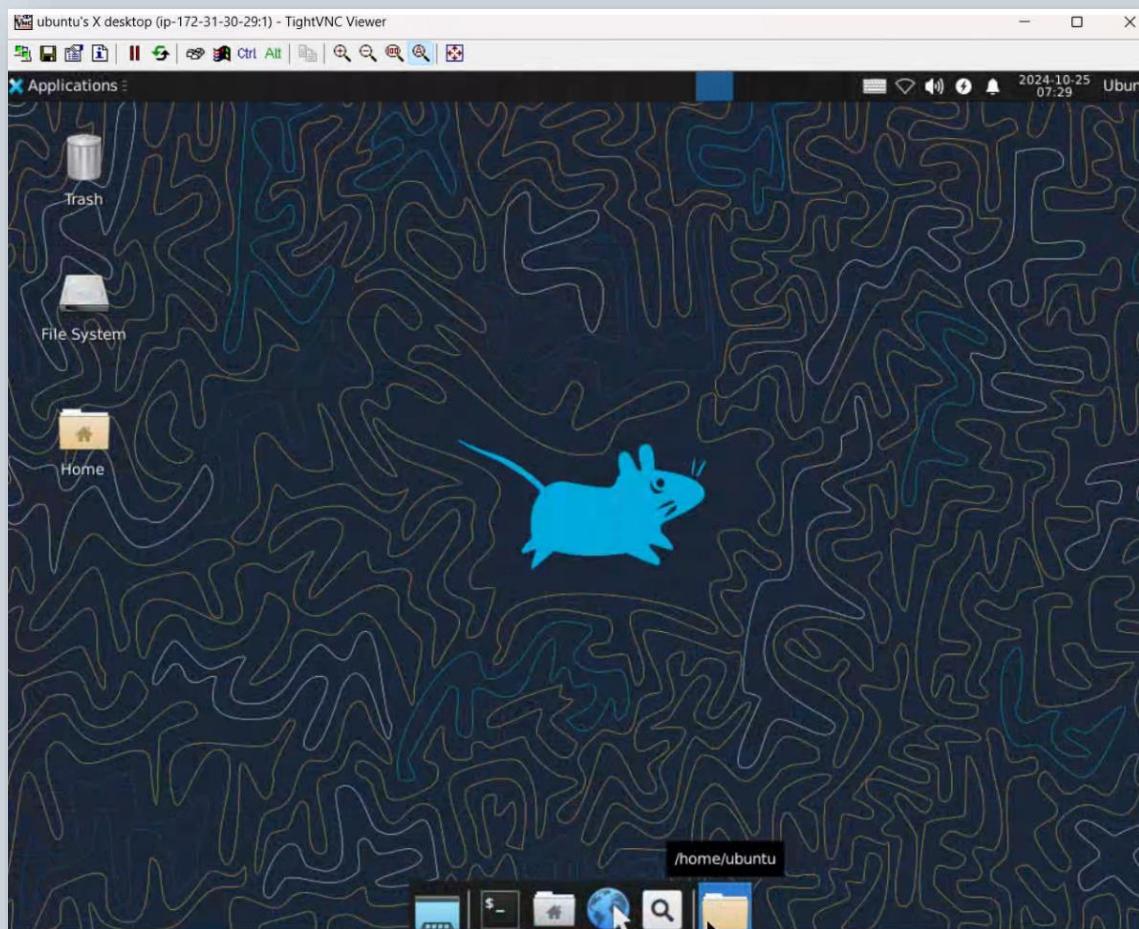
0 updates can be applied immediately.

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Fri Oct 25 06:57:31 2024 from 217.61.224.242
sergio1@ip-172-31-30-29:~$
```

- Abrimos el cliente VNC en el equipo local ingresando localhost:5901 y hacemos el login.





12. Creación de túnel inverso

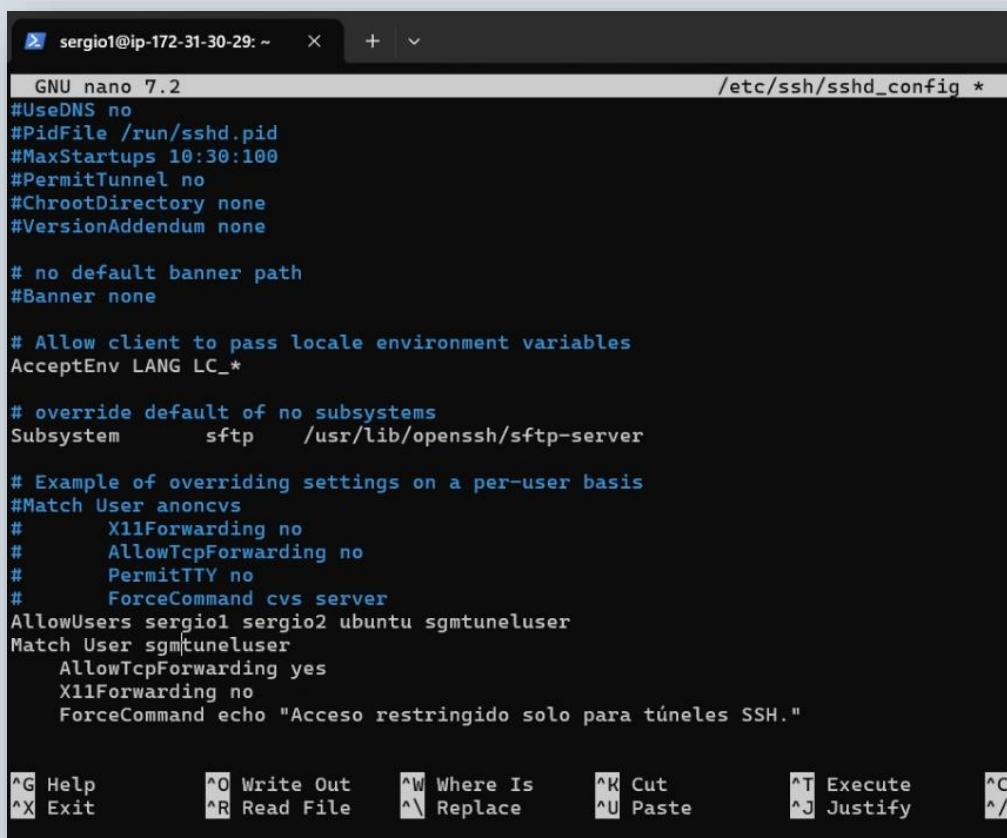
La creación de un túnel inverso es una técnica útil para acceder a dispositivos o servicios en una red privada desde el exterior. Esta configuración se llama "túnel inverso" porque, a diferencia de un túnel SSH tradicional (donde te conectas desde tu máquina local a un puerto remoto), en el túnel inverso el dispositivo remoto crea una conexión SSH hacia tu máquina local, permitiendo el acceso de la red externa al dispositivo remoto a través de tu máquina local.

Con un túnel inverso, puedes acceder de forma segura a dispositivos remotos que están en redes privadas sin necesidad de abrir puertos en el firewall. Esto evita exponer directamente estos dispositivos a internet, reduciendo riesgos de seguridad. Esto es muy útil a la hora de acceder de forma remota y administrar (que es de lo que va este grado en teoría).

Para realizar el túnel inverso, lo primero que hice fue crear un usuario específico para hacer de túnel. En principio lo puse sin contraseña, aunque luego se la agregué igual.

```
sergio1@ip-172-31-30-29:~$ sudo adduser --disabled-password sgmtuneluser
info: Adding user 'sgmtuneluser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group 'sgmtuneluser' (1004) ...
info: Adding new user 'sgmtuneluser' (1004) with group 'sgmtuneluser (1004)' ...
info: Creating home directory '/home/sgmtuneluser' ...
info: Copying files from '/etc/skel' ...
Changing the user information for sgmtuneluser
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 'sgmtuneluser' to supplemental / extra groups 'users' ...
info: Adding user 'sgmtuneluser' to group 'users' ...
sergio1@ip-172-31-30-29:~$
```

Posteriormente, permitiremos el login del usuario y pondremos lo siguiente para que pueda hacer de túnel inverso:



```
sergio1@ip-172-31-30-29: ~      +  ~
GNU nano 7.2                                /etc/ssh/sshd_config *

#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

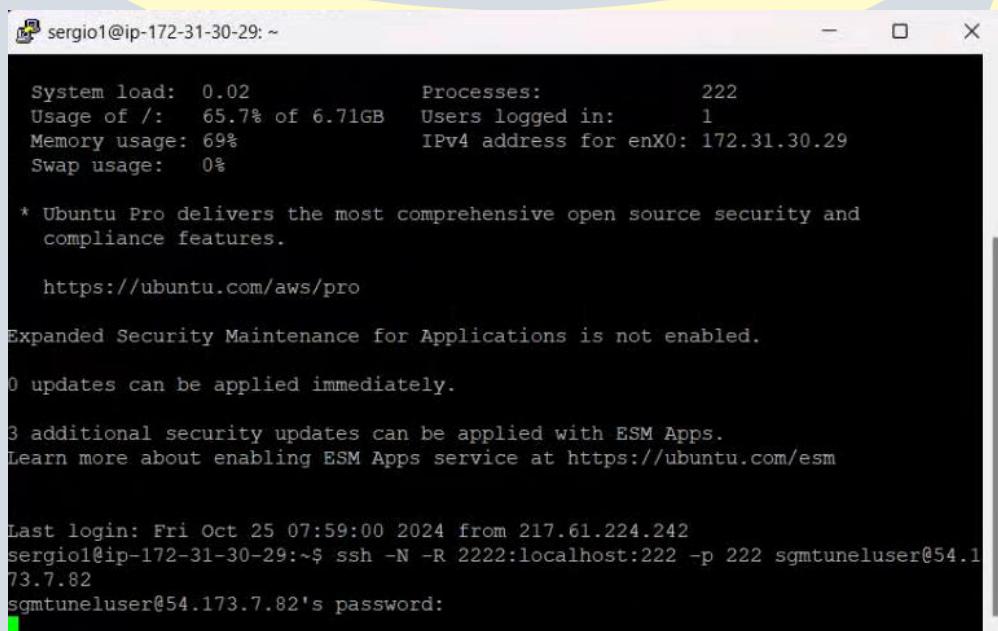
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem    sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
AllowUsers sergio1 sergio2 ubuntu sgmtuneluser
Match User sgmtuneluser
    AllowTcpForwarding yes
    X11Forwarding no
    ForceCommand echo "Acceso restringido solo para túneles SSH."

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute      ^C
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify      ^/
^/
```

A continuación, haremos el siguiente comando para habilitar dicho túnel.



```
sergio1@ip-172-31-30-29: ~
System load:  0.02          Processes:            222
Usage of /:   65.7% of 6.71GB  Users logged in:      1
Memory usage: 69%           IPv4 address for enX0: 172.31.30.29
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.

0 updates can be applied immediately.

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Fri Oct 25 07:59:00 2024 from 217.61.224.242
sergio1@ip-172-31-30-29:~$ ssh -N -R 2222:localhost:222 -p 222 sgmtuneluser@54.1
73.7.82
sgmtuneluser@54.173.7.82's password:
```

Para comprobar que el puerto habilitado 2222 está escuchando desde el localhost, podemos hacer lo siguiente.

```
sergiol@ip-172-31-30-29:~$ netstat -tuln | grep 2222
tcp        0      0 127.0.0.1:2222          0.0.0.0:*
tcp6       0      0 ::1:2222              ::*:*
sergiol@ip-172-31-30-29:~$
```

Ahora podremos hacer ssh -p 2222 sergiol@localhost y podremos hacer el túnel inverso.

```
sergiol@ip-172-31-30-29:~$ ssh -p 2222 sergiol@localhost
Welcome to Ubuntu 24.04.1 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 Fri Oct 25 08:08:26 UTC 2024

System load:  0.01           Processes:            228
Usage of /:   65.7% of 6.71GB  Users logged in:     1
Memory usage: 69%
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.

0 updates can be applied immediately.

3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Fri Oct 25 08:08:27 2024 from 217.61.224.242
sergiol@ip-172-31-30-29:~$ exit
```

Si paramos el comando del usuario sgmtuneluser, podemos comprobar que nos saca del acceso remoto por túnel inverso.

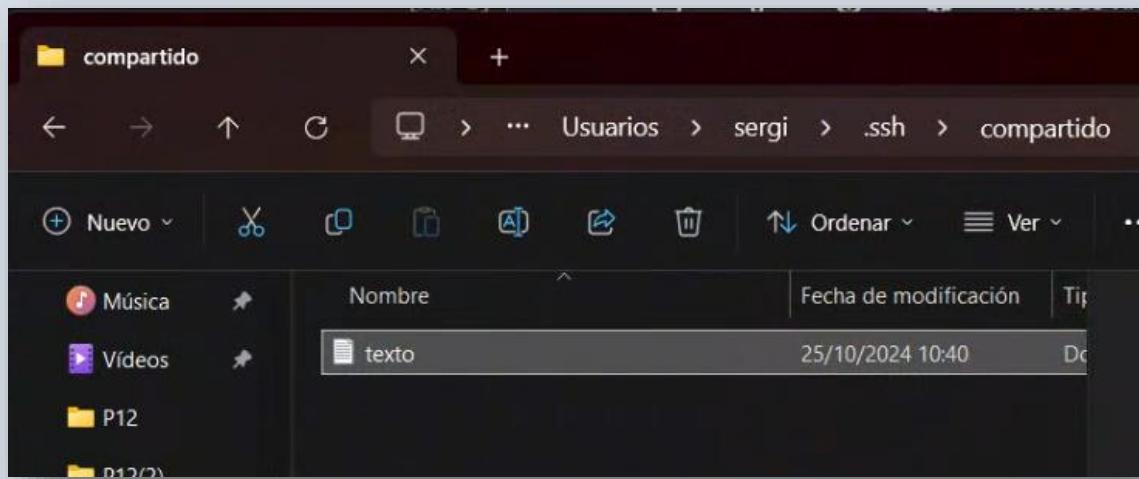


```
sergio1@ip-172-31-30-29: ~
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Fri Oct 25 08:07:43 2024
System load: 0.02
Usage of /: 65.7% of 6.71GB
Memory usage: 69%
Swap usage: 0%
* Ubuntu Pro delivers the most comprehensive open source security and compliance features.
https://ubuntu.com/aws/pro
xpanded Security Maintenance for Applications can be applied immediately. Additional security updates can be applied with ESM Apps. Learn more about enabling ESM Apps service at https://ubuntu.com/esm
ast login: Fri Oct 25 07:59:00 2024
sergio1@ip-172-31-30-29: ~ ssh -L 37.82 gmtuneluser@54.173.7.82's password:
Csergio1@ip-172-31-30-29: ~
ígenes
I
álogo de AMI
Direcc
Last login: Fri Oct 25 08:07:43 2024 from 127.0.0.1
sergio1@ip-172-31-30-29: ~$ ssh -p 2222 sergio1@localhost
Welcome to Ubuntu 24.04.1 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 Fri Oct 25 08:08:26 UTC 2024
System load: 0.01      Processes: 228
Usage of /: 65.7% of 6.71GB  Users logged in: 1
Memory usage: 69%      IPv4 address for enX0: 172.31.30.29
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.
0 updates can be applied immediately.
3 additional security updates can be applied with ESM Apps. Learn more about enabling ESM Apps service at https://ubuntu.com/esm
Last login: Fri Oct 25 08:08:27 2024 from 217.61.224.242
sergio1@ip-172-31-30-29: ~$ exit
Connection to localhost closed.
Connection to localhost closed.
```

13. Transferir archivos desde tu máquina local a la instancia EC2 utilizando SCP.

Para transferir el archivo, lo primero que he hecho es crear una carpeta con un archivo de prueba.



Una vez lo tenemos, vamos a PowerShell, sin estar en la máquina virtual, y copiaremos el texto a nuestro server.

```
PS C:\Users\sergi\.ssh> scp -P 222 .\compartido\texto.txt sergio1@54.173.7.82:/tmp/
Load key "C:\\\\Users\\\\sergi/.ssh/id_rsa": invalid format
sergio1@54.173.7.82's password:
texto.txt                                              100%   45      0.3KB/s   00:00
PS C:\Users\sergi\.ssh> |
```

Si salió bien, iremos al server y veremos que el archivo se copió correctamente.

```
sergio1@ip-172-31-30-29:/tmp$ cat texto.txt
Esto es un texto de la práctica 12 de sergio1@ip-172-31-30-29:/tmp$
```

14. Transferir archivos desde la instancia a tu máquina local a la utilizando SCP

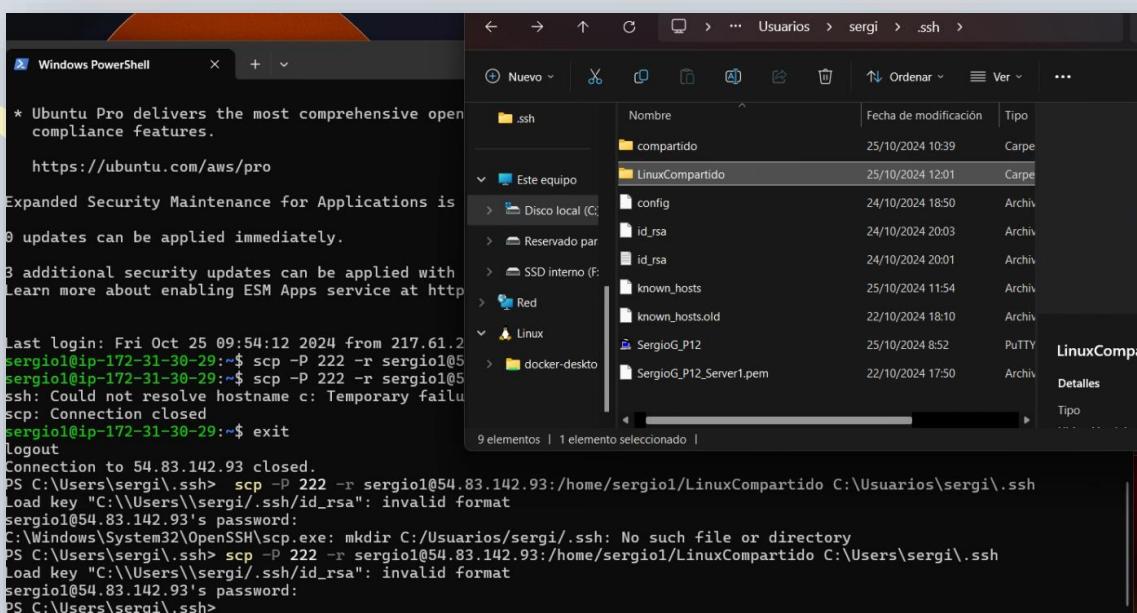
Ahora haremos el camino inverso, del host a la instancia. Para ello me he creado la carpeta y archivos que aparecen a continuación.

```
sergio1@ip-172-31-30-29:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos snap
sergio1@ip-172-31-30-29:~$ mkdir LinuxCompartido
sergio1@ip-172-31-30-29:~$ touch ejemplo.txt
sergio1@ip-172-31-30-29:~$ |
```

Ponemos el comando siguiente y se compartirá.

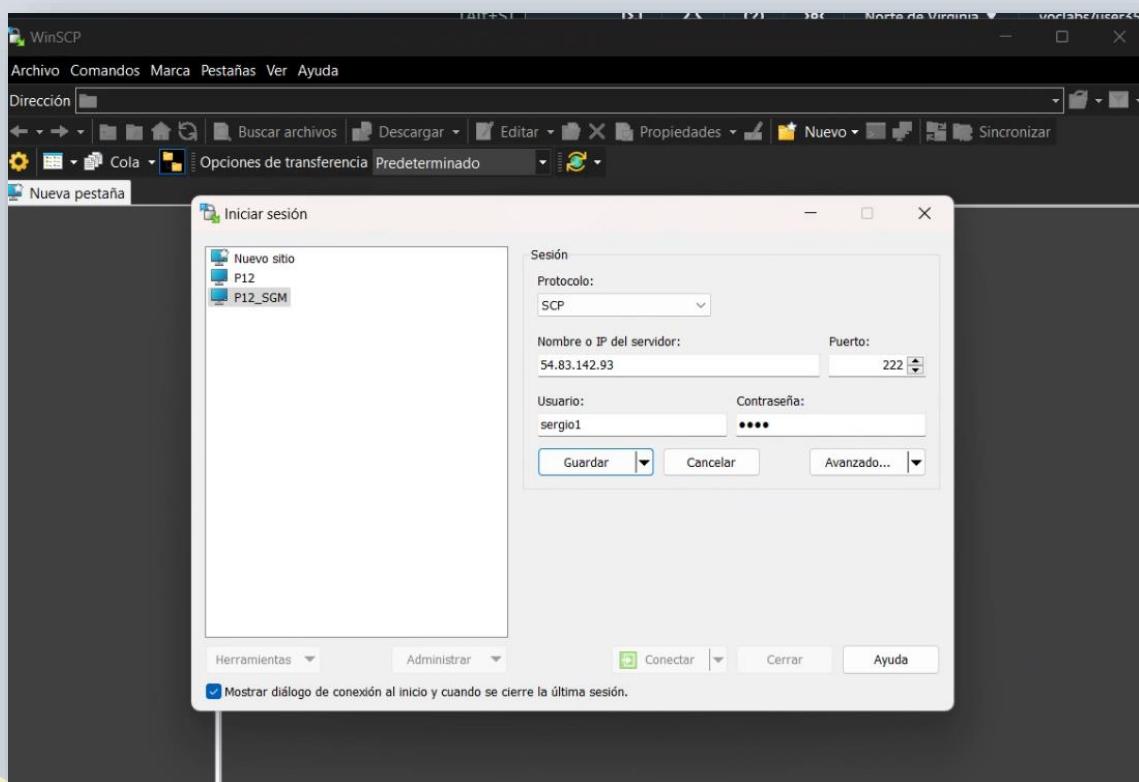
```
PS C:\Users\sergi\.ssh> scp -P 222 -r sergio1@54.83.142.93:/home-sergio1/LinuxCompartido C:\Users\sergi\.ssh
Load key "C:\\\\Users\\\\sergi\\\\.ssh\\\\id_rsa": invalid format
sergio1@54.83.142.93's password:
PS C:\Users\sergi\.ssh> |
```

Con esto, ya tendríamos compartida la carpeta y todo listo.

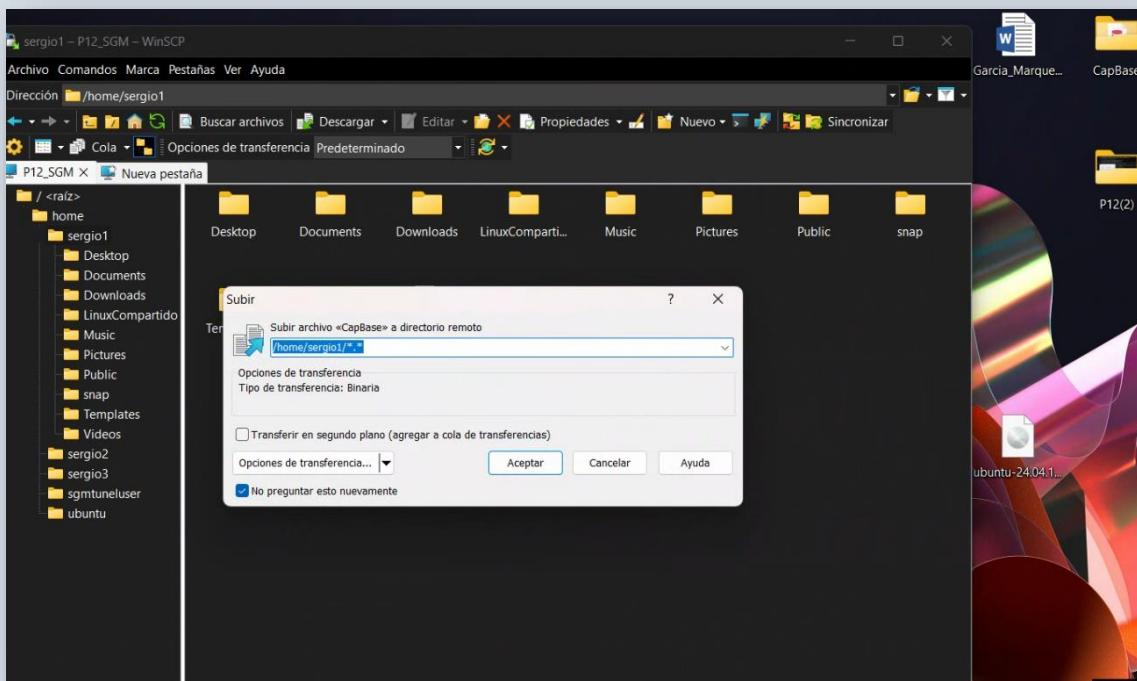


15. Subir archivos a un servidor por SSH con WinSCP

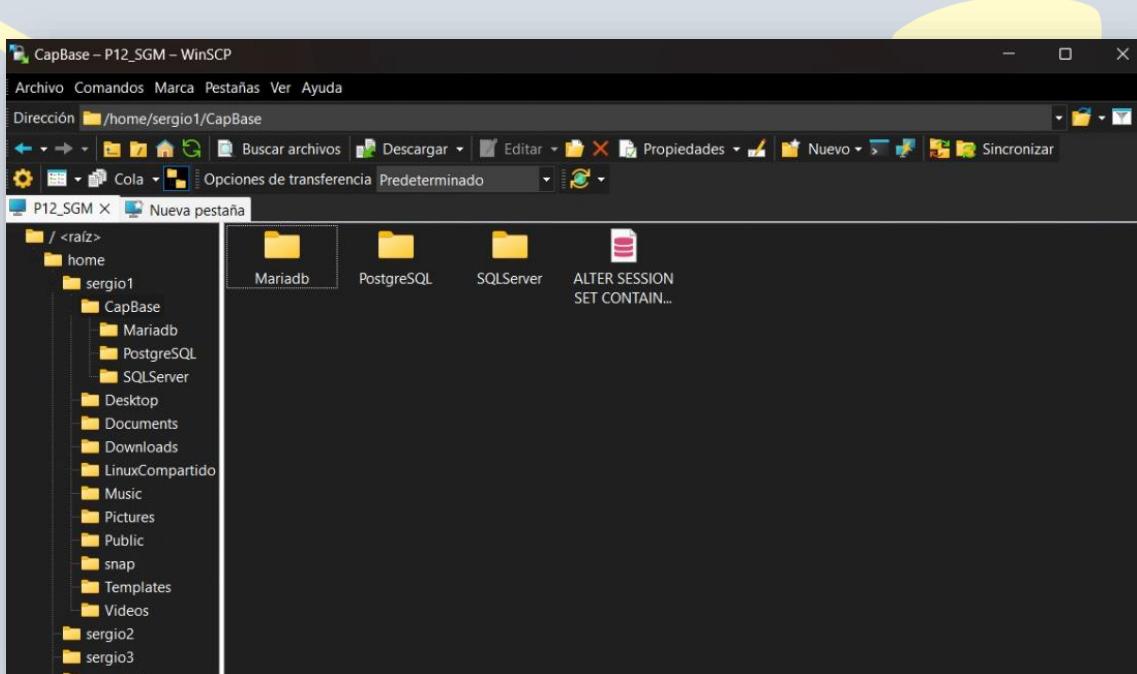
Para conectarnos a la instancia por WinSCP, lo primero es usar el protocolo SCP, poner la IP pública, el puerto y el usuario con su contraseña.



Con esta configuración, ya podremos conectarnos. Ahora podremos probar a añadir archivos simplemente arrastrándolos.

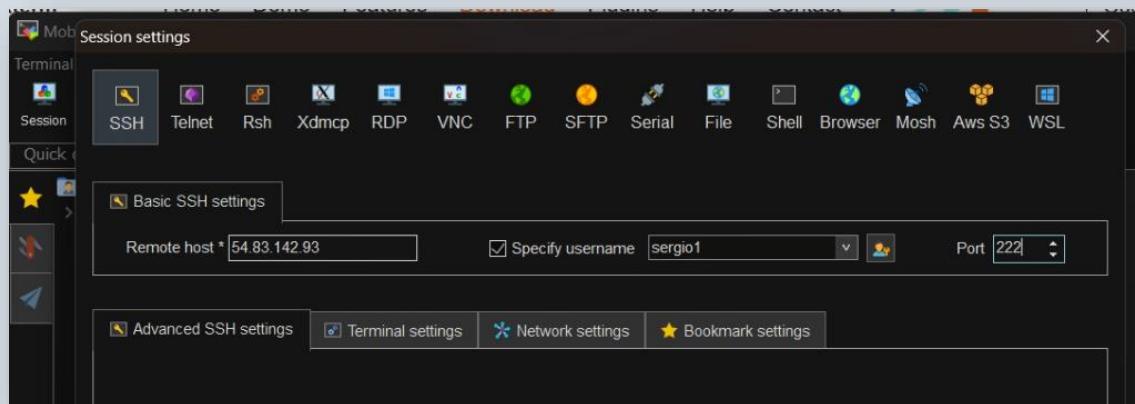


Esperamos y ya tendríamos listo el archivo.



16. Transferencia de archivos desde Mobxterm

Lo primero será conectarnos por la aplicación.

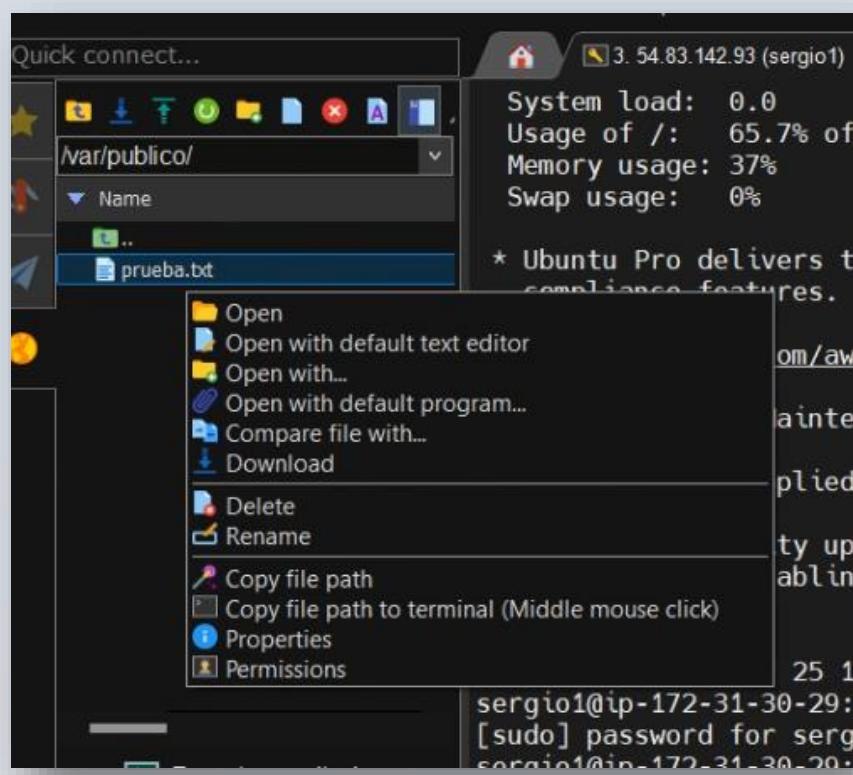


Creamos con nano un archivo en el servidor en /var/publico/prueba.txt

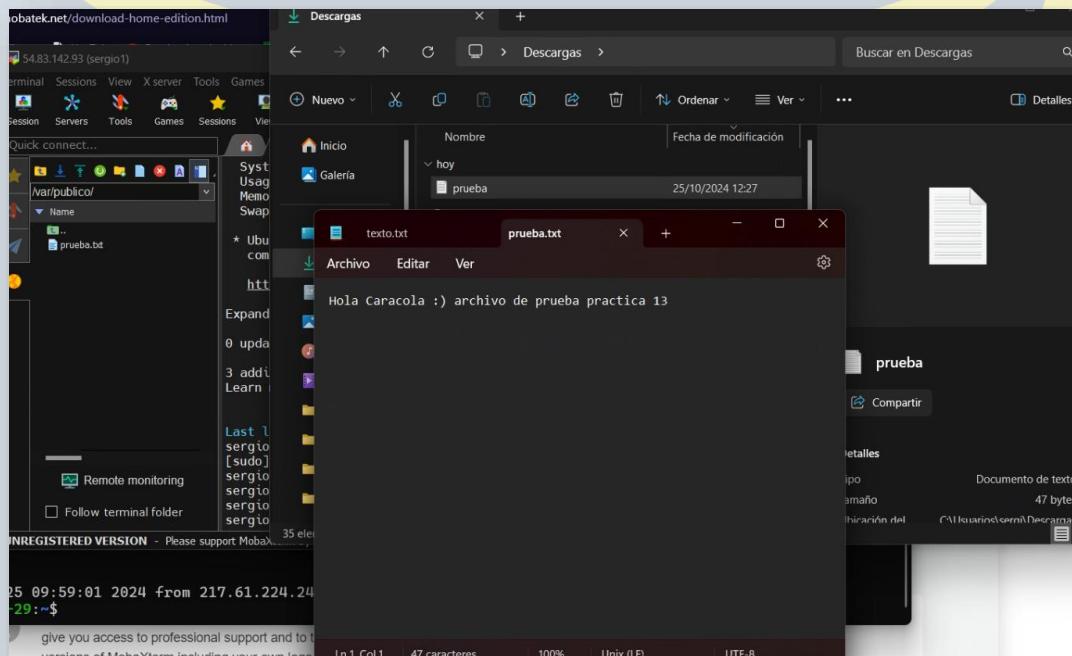
```
System information as of Fri Oct 25 10:22:09 UTC 2024
System load: 0.0          Processes:      150
Usage of /: 65.7% of 6.71GB  Users logged in: 1
Memory usage: 37%          IPv4 address for enX0: 172.31.30.29
Swap usage: 0%
* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.
https://ubuntu.com/aws/pro
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
3 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Fri Oct 25 10:04:53 2024 from 217.61.224.242
sergio1@ip-172-31-30-29:~$ sudo mkdir -p /var/publico
[sudo] password for sergio1:
sergio1@ip-172-31-30-29:~$ sudo nano /var/publico/prueba.txt
Port MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
```

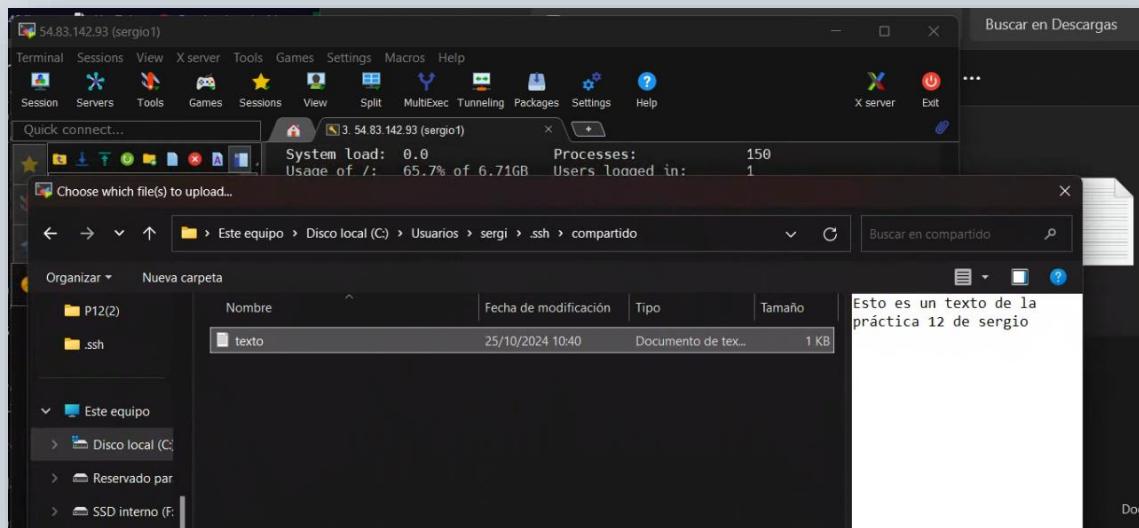
Ya tenemos el archivo para jugar con él. Lo primero que probaremos, será descargarlo, le damos clic derecho y le damos a download.



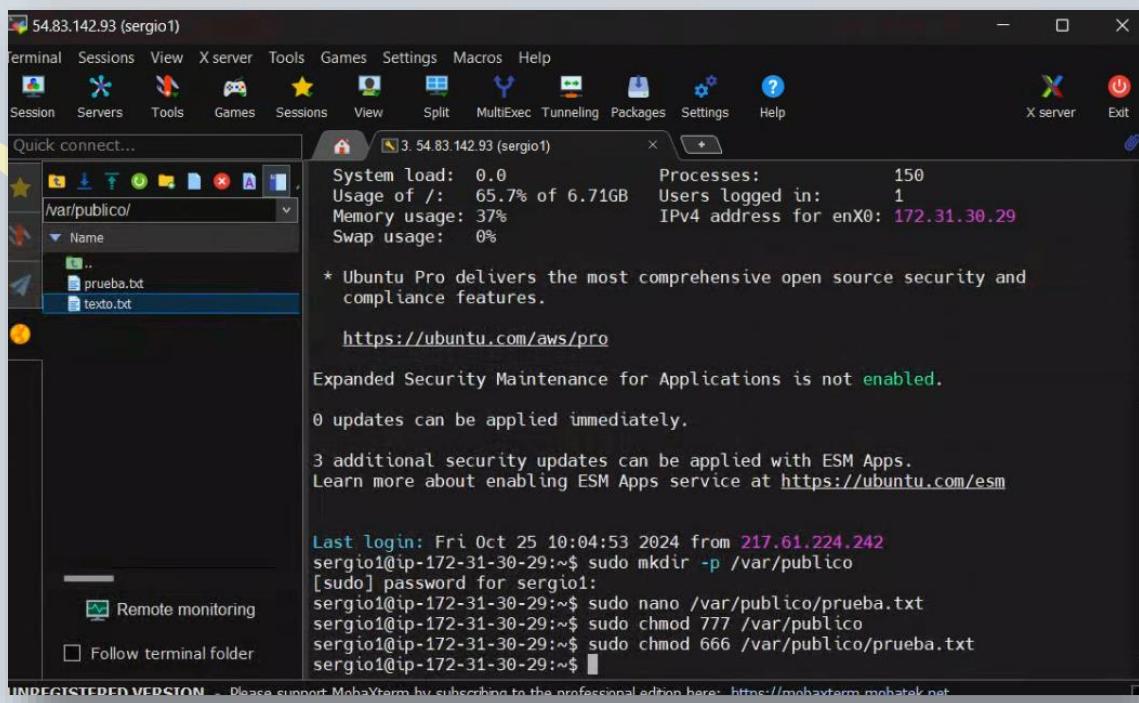
En la carpeta de descargas debería aparecer dicho archivo.



Ahora probaremos la inversa. Cogemos un archivo de puntos anteriores.



Volvemos a la aplicación y le damos ala flechita azul, que su función es “upload”.
Cogemos el archivo.



17. Transferir archivos desde la instancia a tu máquina local a la utilizando SFTP

Para entrar en sftp, debemos poner el siguiente comando:

```
sftp> PS C:\Users\sergi\.ssh> sftp -i .\SergioG_P12_Server1.pem -o Port=222 sergio1@ec2-54-83-142-93.compute-1.amazonaws.com  
sergio1@ec2-54-83-142-93.compute-1.amazonaws.com's password:  
Connected to ec2-54-83-142-93.compute-1.amazonaws.com.  
sftp>
```

Una vez dentro del servidor solo bastará ejecutar el comando “get” para descargar algún fichero o archivo del servidor remoto al equipo local. El comando “put” para copiar algún fichero o archivo local al servidor remoto.

Podemos explorar el sistema de archivos un poco y ver que estamos en la máquina con el usuario sergio1.

```
sftp> PS C:\Users\sergi\.ssh> sftp -i .\SergioG_P12_Server1.pem -o Port=222 sergio1@ec2-54-83-142-93.compute-1.amazonaws.com  
sergio1@ec2-54-83-142-93.compute-1.amazonaws.com's password:  
Connected to ec2-54-83-142-93.compute-1.amazonaws.com.  
sftp> ls  
CapBase Desktop Documents Downloads LinuxCompartido Music Pictures  
Public Templates Videos ejemplo.txt snap  
sftp>
```

```
sftp> PS C:\Users\sergi\.ssh> sftp -i .\SergioG_P12_Server1.pem -o Port=222 sergio1@ec2-54-83-142-93.compute-1.amazonaws.com  
sergio1@ec2-54-83-142-93.compute-1.amazonaws.com's password:  
Connected to ec2-54-83-142-93.compute-1.amazonaws.com.  
sftp> ls  
CapBase Desktop Documents Downloads LinuxCompartido Music Pictures  
Public Templates Videos ejemplo.txt snap  
sftp> cd LinuxCompartido  
sftp> ls  
sftp> |
```

```
sftp> ls /home/sergio1/Downloads/  
/home/sergio1/Downloads/prueba2.txt  
sftp>
```

Ahora podemos probar a subir un archivo SFTP.

```
sftp> get prueba2.txt
Fetching /home/sergio1/Downloads/prueba2.txt to prueba2.txt
prueba2.txt
sftp>
```

menes Nombre de IP: ip-172-31-30-29.ec2.internal ip-172-31-30-29.ec2.internal

100% 47 0.2KB/s

Y también probar a descargar un archivo desde la instancia.

```
sftp> get C:\Users\sergi\Downloads\prueba2.txt
File "/C:/Users/sergi/Downloads/prueba2.txt" not found.
sftp> ls /home/sergio1/Downloads/
/home/sergio1/Downloads/prueba2.txt
sftp> get prueba2.txt
Fetching /home/sergio1/Downloads/prueba2.txt to prueba2.txt
prueba2.txt
sftp> exit
PS C:\Users\sergi\.ssh>
```

