SEGUNDA PRÁCTICA -CONEXIÓN CLIENTE SERVIDOR POR SSH CON CLAVE PÚBLICA

Las máquinas tendrán la siguiente configuración:

Servidor:

Ip → 192.168.42.2 /24

Cliete:

Ip → 192.168.42.7 /24

Conexión del cliente al servidor sin contraseña.

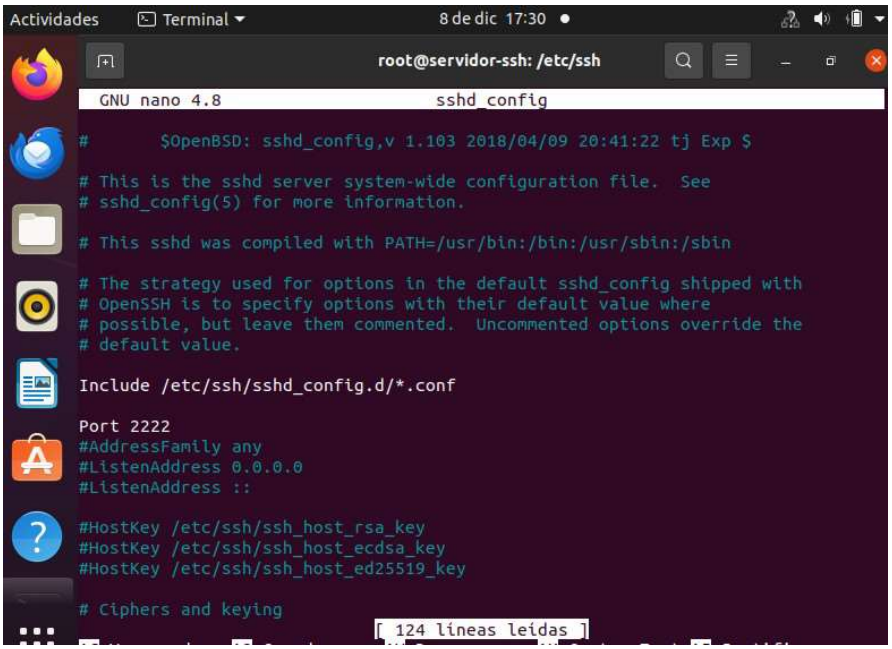
PASOS:

1. **Configuración de Ips en el cliente y en el servidor.**
   Muestra con el comando correspondiente que el servidor y cliente tienen la IP que se pide

```
root@servidor-ssh:/etc/ssh# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt 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 g
roup default qlen 1000
    link/ether 08:00:27:4d:ee:ae brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.2/24 brd 192.168.42.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::276f:afb0:33e4:1486/64 scope link dadfailed tentative noprefixr
oute
       valid_lft forever preferred_lft forever
    inet6 fe80::7934:5518:de48:73c5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:ab:a2:1d brd ff:ff:ff:ff:ff:ff
root@servidor-ssh:/etc/ssh#
```

```
gracia@cliente-ssh:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
lt 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
roup default qlen 1000
    link/ether 08:00:27:06:d0:3d brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.7/24 brd 192.168.42.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::276f:afb0:33e4:1486/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
roup default qlen 1000
    link/ether 08:00:27:ac:d2:02 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::cd97:9ed7:35e0:9032/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

2. **Se conectarán por el puerto 2222, cambialo en el fichero de configuración.**



3. **Para la conexión sin contraseña o clave pública se seguirán los siguientes puntos:**

A) Se generará en la máquina cliente una clave pública.

ssh-keygen -t rsa

Se trata de un proceso interactivo de generación de claves y por ello se hacen algunas preguntas, como:

• Escribe el nombre del archivo en el que guardarás la clave (~/.ssh/id_rsa)

• Escribe la passphrase (vacía si quieres dejarlo sin passphrase)

Se puede presionar Intro para ambas preguntas y el sistema tomará los valores predeterminados.

```
root@cliente-ssh:/home/gracia# ssh-keygen -t rsa
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
T LibreOffice Writer int is:
SHA256:99SH5nKFhP+eOyWb9h6Bh2hjHPtjiK9R34sNelliZSk root@cliente-ssh
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|              .  |
|           .. . .|
|          . +Eo* |
|        S .O.oXoo|
|         .=o==+=o|
|         o .+***o|
|          o o=Oo+|
|         ..o.o B*|
+----[SHA256]-----+
root@cliente-ssh:/home/gracia#
```

B) Copiar la clave que se ha generado en la máquina Servidor.

ssh-copy-id remote_username@remote_IP_Address

```
gracia@cliente-ssh:~$ sudo ssh-copy-id -p 2222 gracia@192.168.42.2
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rs
a.pub"
The authenticity of host '[192.168.42.2]:2222 ([192.168.42.2]:2222)' can't be e
stablished.
ECDSA key fingerprint is SHA256:pVWLB8QNbhwFpg50lBrUk0aVUB8dTePXdTnP94nl5ew.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/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 promp
ted now it is to install the new keys
gracia@192.168.42.2's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -p '2222' 'gracia@192.168.42.2'"
and check to make sure that only the key(s) you wanted were added.
```

C) Nos conectamos a la máquina servidor

```
gracia@cliente-ssh:~$ sudo ssh -p 2222 gracia@192.168.42.2
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

El mantenimiento de seguridad expandido para Infrastructure está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

108 actualizaciones de seguridad adicionales se pueden aplicar con ESM Infra.
Aprenda más sobre cómo activar el servicio ESM Infra for Ubuntu 20.04 at
https://ubuntu.com/20-04

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
 Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Dec  8 16:25:32 2025 from 192.168.5.2
gracia@servidor-ssh:~$
```

Solamente tendrá que pedirme la clave la primera vez.

D) Para comprobarlo:

1º) Desde la máquina Cliente me desconecto del Servidor

```
gracia@servidor-ssh:/home$ exit
logout
Connection to 192.168.42.2 closed.
```

2º) Volveré a conectarme, para que el ejercicio esté correcto la segunda vez que me conecto no debe pedirme la contraseña.

```
gracia@cliente-ssh:~$ sudo ssh -p 2222 gracia@192.168.42.2
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

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

El mantenimiento de seguridad expandido para Infrastructure está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

108 actualizaciones de seguridad adicionales se pueden aplicar con ESM Infra.
Aprenda más sobre cómo activar el servicio ESM Infra for Ubuntu 20.04 at
https://ubuntu.com/20-04

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
 Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Dec  8 17:59:04 2025 from 192.168.42.7
gracia@servidor-ssh:~$
```