CONEXIÓN CLIENTE SERVIDOR POR SSH CON CLAVE PÚBLICA

REALIZADO POR: ALEJANDRO GUERRA ABÁN | IES MELCHOR GASPAR DE JOVELLANOS | SMR2A

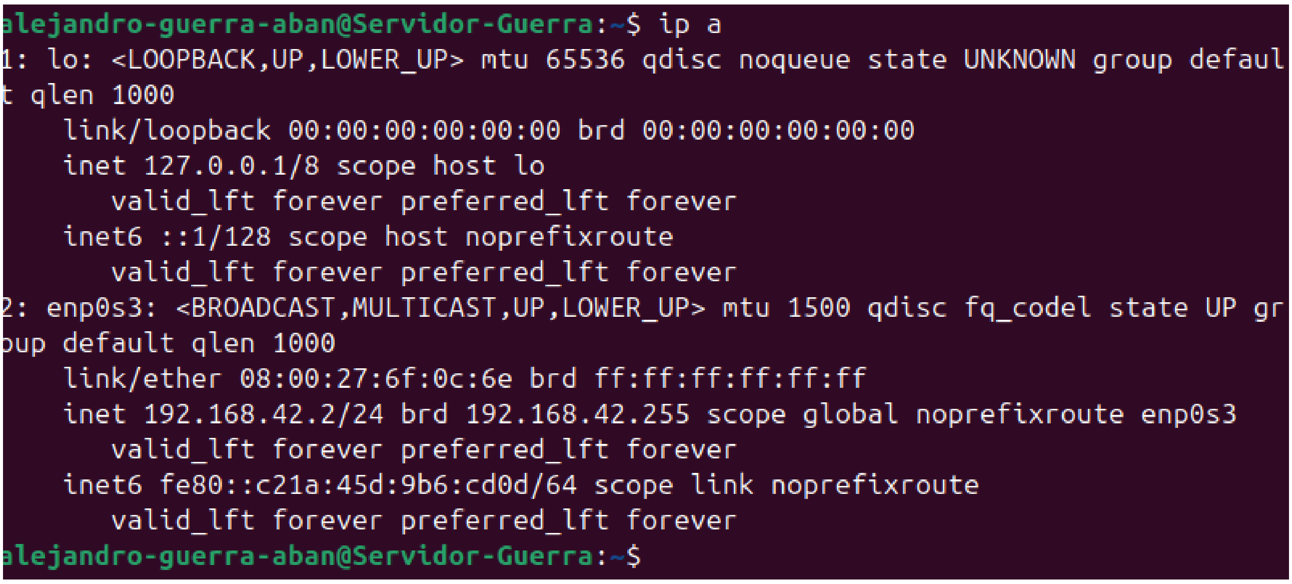
INDICE

adictosalinux.com
> CONFIGURAR
> SSH
> SIN CONTRASEÑA
#Linux #SSH #Servidores

PASOS PREVIOS

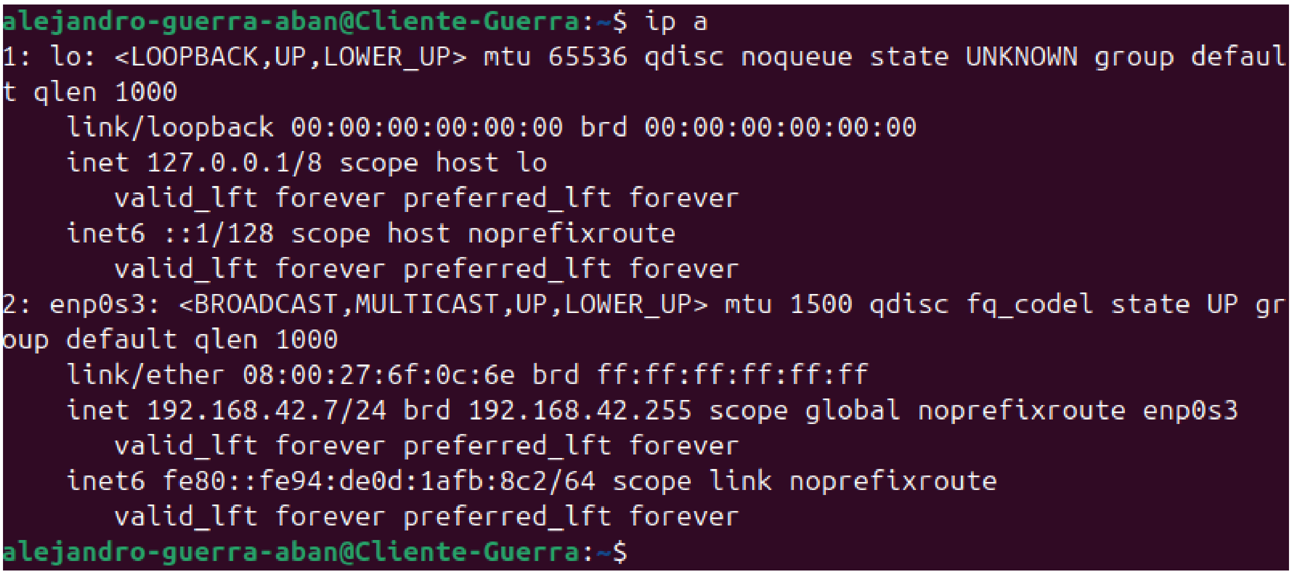
CAMBIAMOS / AJUSTAMOS las IP’S de cada maquina para realizar la tarea

SERVIDOR:



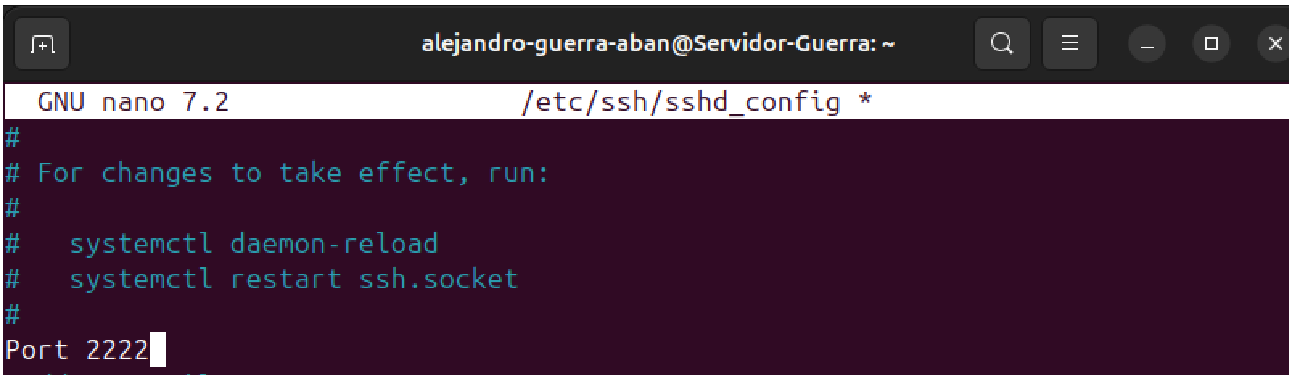
```
alejandro-guerra-aban@Servidor-Guerra:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:6f:0c:6e 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::c21a:45d:9b6:cd0d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
alejandro-guerra-aban@Servidor-Guerra:~$
```

CLIENTE:



```
alejandro-guerra-aban@Cliente-Guerra:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:6f:0c:6e 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::fe94:de0d:1afb:8c2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
alejandro-guerra-aban@Cliente-Guerra:~$
```

Cambiamos el puerto del servicio al 2222 que se indica para poder realizar la práctica

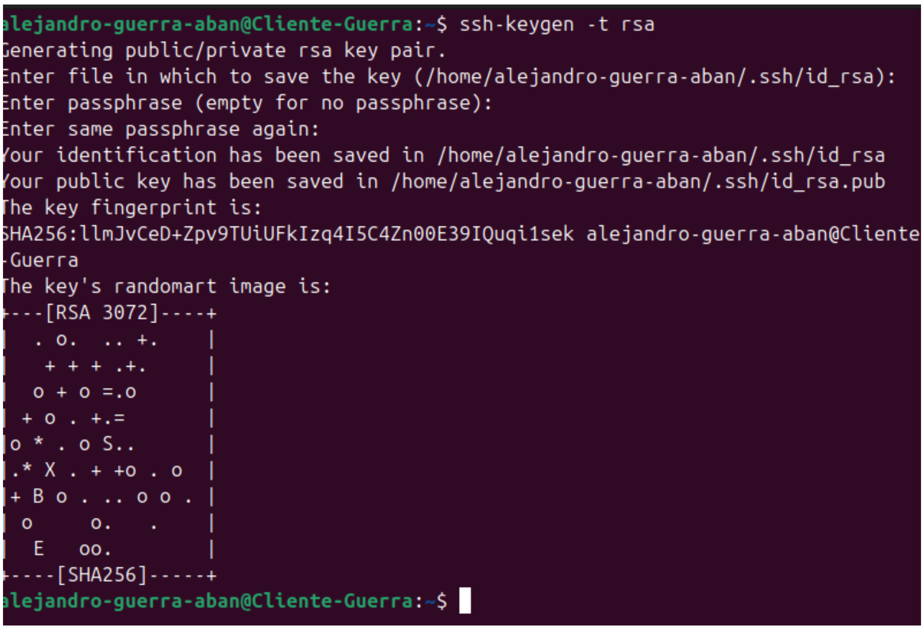


```
  GNU nano 7.2                  /etc/ssh/sshd_config *
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
Port 2222
```

CONFIGURACIÓN

① Generar una clave pública. Para generar una clave pública y privada se usa el comando: ssh-keygen -t rsa

Usamos este comando para generar la clave publica para conectarnos de forma más segura al servidor.



```
alejandro-guerra-aban@Cliente-Guerra:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/alejandro-guerra-aban/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alejandro-guerra-aban/.ssh/id_rsa
Your public key has been saved in /home/alejandro-guerra-aban/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:llmJvCeD+Zpv9TUiUFkIzq4I5C4Zn00E39IQuqi1sek alejandro-guerra-aban@Cliente
-Guerra
The key's randomart image is:
+---[RSA 3072]----+
|  . o.  .. +.    |
|   + + + .+.     |
|  o + o =.o      |
| + o . +.=       |
|o * . o S..      |
|.* X . + +o . o  |
|+ B o . .. o o . |
| o     o.   .    |
|  E   oo.        |
+----[SHA256]-----+
alejandro-guerra-aban@Cliente-Guerra:~$
```

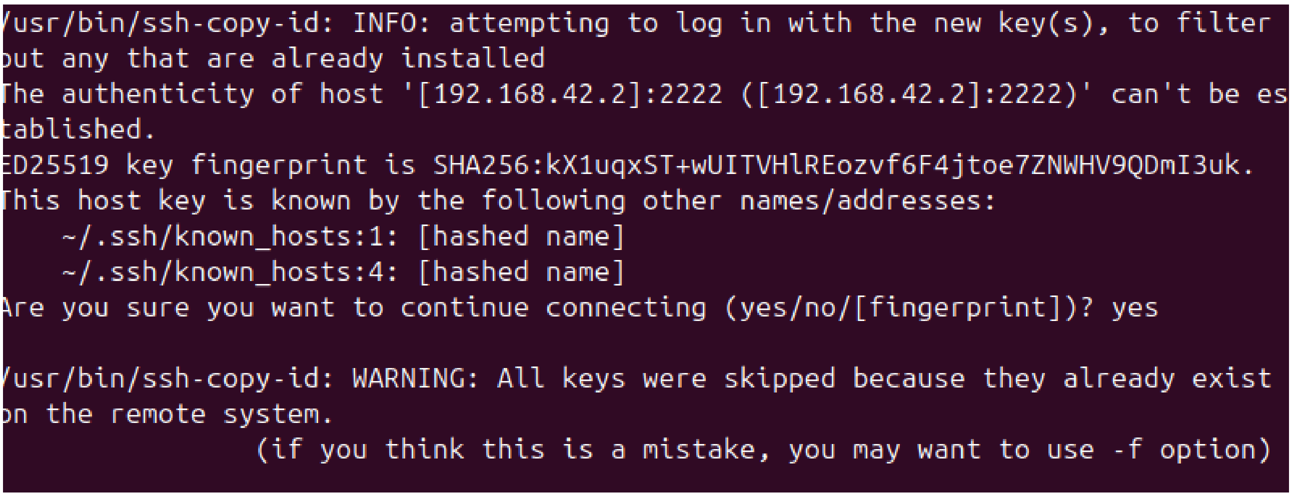
② Copiar la clave que se ha generado en el paso 1.

Por si acaso es recomendable guardar la contraseña en un lugar externo y seguro.

xolHnHdzhCQjsPlEpc7f7Lv/0Ovsvi7kifVWTH7qCfE

Al usar el comando ssh-copy-id remote_user@ip_remote

Añadirá la clave que hemos generado antes para que no nos la vuelva a pedir la próxima vez que nos conectemos por SSH

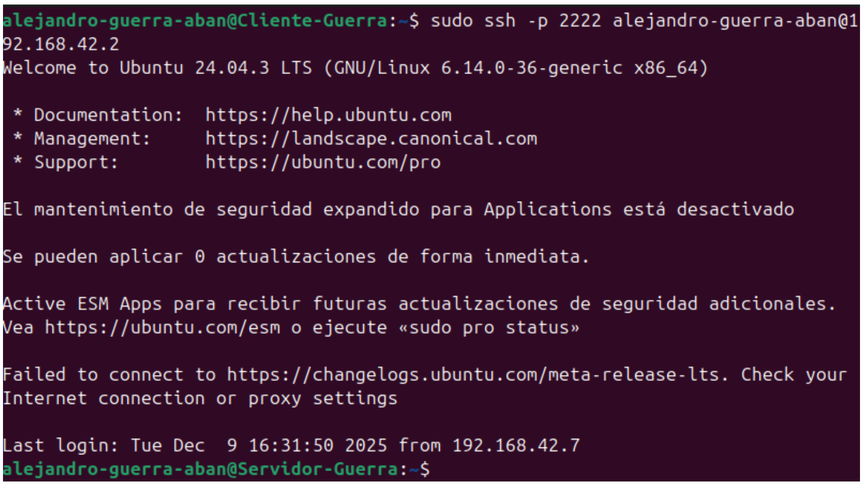


```
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
The authenticity of host '[192.168.42.2]:2222 ([192.168.42.2]:2222)' can't be es
tablished.
ED25519 key fingerprint is SHA256:kX1uqxST+wUITVHlREozvf6F4jtoe7ZNWHV9QDmI3uk.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

/usr/bin/ssh-copy-id: WARNING: All keys were skipped because they already exist
on the remote system.
                (if you think this is a mistake, you may want to use -f option)
```

COMPROBACIONES FINALES:

Podemos observar que la primera que nos pedirá una contraseña y después al desconectarnos y al volver a conectarnos ya nos la volverá pedir la contraseña



```
alejandro-guerra-aban@Cliente-Guerra:~$ sudo ssh -p 2222 alejandro-guerra-aban@1
92.168.42.2
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-36-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

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

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

Last login: Tue Dec  9 16:31:50 2025 from 192.168.42.7
alejandro-guerra-aban@Servidor-Guerra:~$
```