



SSH EN UBUNTU SERVER

SRI



2ºASIR
I.E.S. ANTONIO MACHADO
ANA OROZCO ASENSIO

Contenido

IP.....	2
Instalación.....	3
Acceder por SSH.....	3
Usa el explorador de carpetas de los clientes linux y windows para acceder al servidor ssh.....	6
Usa el comando scp para copiar ficheros a/desde el servidor ssh	7
Configura el servidor ssh para conectarse mediante certificado digital en lugar de usuario/password.	8
Crea túneles ssh para conectarte de manera segura a los distintos servicios del servidor.....	9

IP.

Para cambiar la IP en modo comando haremos:

```
sudo nano /etc/netplan/01-netcfg.yaml
```

Para aplicarlo haremos

```
Sudo netplan apply
```

```
ana@ana:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8d:6b:b9 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.98/24 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe8d:6bb9/64 scope link
            valid_lft forever preferred_lft forever
ana@ana:~$
```

***Importante:**

hacer sudo apt update y sudo apt upgrade

```
usuario@clientelinux:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:58:46:a9 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.99/21 brd 192.168.7.255 scope global noprefixroute enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::8dcf:67f6:f98b:2ba1/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

Instalación.

Haremos la instalación

```
sudo apt install openssh-server
```

```
ana@ana:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Mon 2024-12-02 18:53:18 UTC; 24s ago
TriggeredBy: • ssh.socket
    Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 10824 (sshd)
    Tasks: 1 (limit: 2276)
   Memory: 2.1M (peak: 2.3M)
      CPU: 25ms
     CGroup: /system.slice/ssh.service
             └─10824 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 02 18:53:18 ana systemd[1]: Starting OpenBSD Secure Shell server...
Dec 02 18:53:18 ana sshd[10824]: Listening on :: port 22
Dec 02 18:53:18 ana sshd[10824]: Connection from 127.0.0.1 port 53212
```

Acceder por SSH.

En Windows:

Abriremos el Símbolo del Sistema y pondremos:

```
Ssh ana@192.168.1.98
```

Una vez cargue nos dirá la key de la huella digital (que es una clave publica en SSH) y nos pedirá si queremos conectarnos aunque no estemos autenticados de forma “oficial”.

Además, nos pedirá la contraseña del usuario al que nos estamos conectando.

Para realizar la comprobación haré ip a en el servidor y también en la conexión ssh.

Servidor:

```

ana@ana:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:8d:6b:b9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.98/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8d:6bb9/64 scope link
        valid_lft forever preferred_lft forever
ana@ana:~$
```

Por SSH:

```

ana@ana:~ ~ + ~
Host key verification failed.

C:\Users\anaor>ssh ana@192.168.1.98
The authenticity of host '192.168.1.98 (192.168.1.98)' can't be established.
ED25519 key fingerprint is SHA256:klSpOLSziA6HOeMzjW9gZv3H5d7dtsv060ut0Ukjs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.98' (ED25519) to the list of known hosts.
ana@192.168.1.98's password:
Permission denied, please try again.
ana@192.168.1.98's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

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

System information as of lun 02 dic 2024 18:56:34 UTC

System load:  0.33          Processes:           103
Usage of /:   39.0% of 11.21GB  Users logged in:      1
Memory usage: 11%           IPv4 address for enp0s3: 192.168.1.98
Swap usage:   0%

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»

ana@ana:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:8d:6b:b9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.98/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8d:6bb9/64 scope link
        valid_lft forever preferred_lft forever
```

Para conectarnos desde Linux Mint (en mi caso), será igual:

```
ana@ana:~ - □
Archivo Editar Ver Buscar Terminal Ayuda
ana@ana-VirtualBox:~$ ssh ana@192.168.1.98
The authenticity of host '192.168.1.98 (192.168.1.98)' can't be established.
ED25519 key fingerprint is SHA256:kLSp0LSziA6H0eMzMZjW9gZv3H5d7dtsv060ut0Ukj5.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.98' (ED25519) to the list of known hosts.
ana@192.168.1.98's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

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

System information as of lun 02 dic 2024 19:39:11 UTC

System load: 0.0          Processes:           104
Usage of /: 39.1% of 11.21GB  Users logged in:      1
Memory usage: 12%          IPv4 address for enp0s3: 192.168.1.98
Swap usage:  0%

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

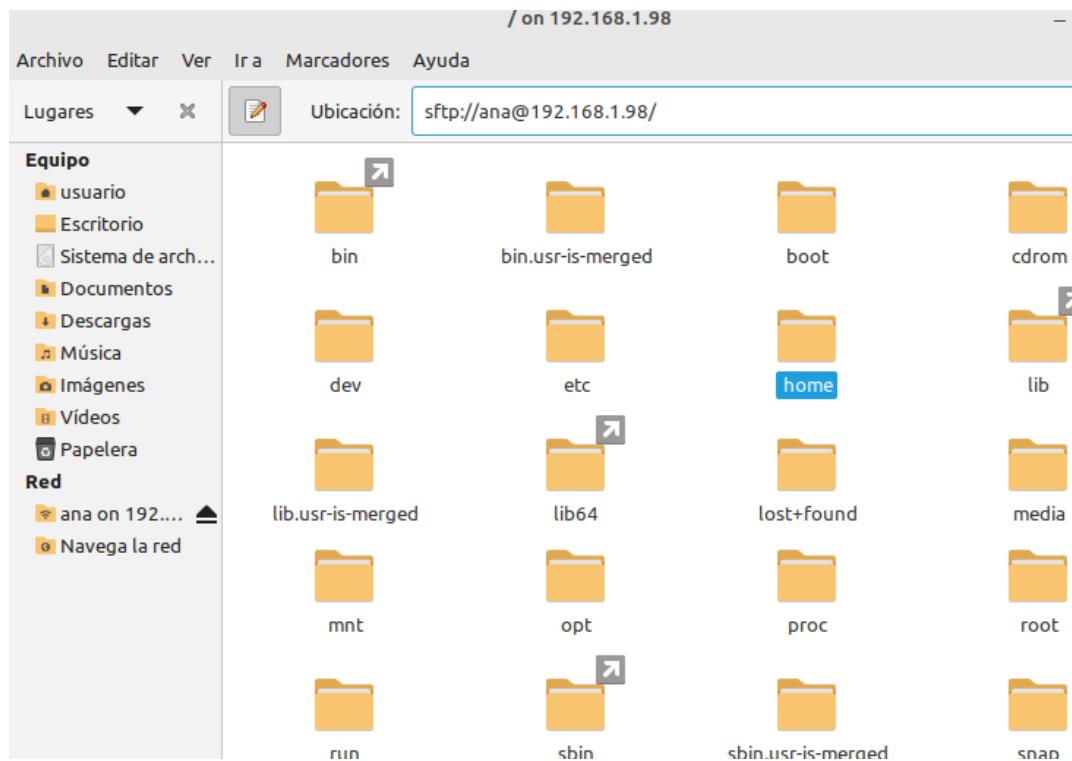
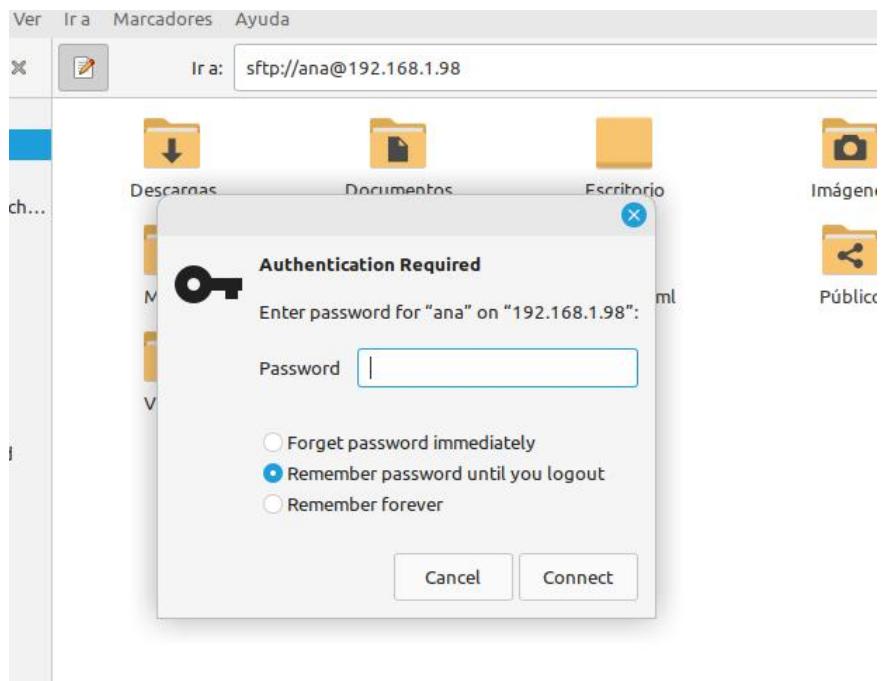
Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


Last login: Mon Dec  2 18:56:34 2024 from 192.168.1.32
ana@ana:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 0
    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 pfifo_fast state UP group 0
    link/ether 08:00:27:8d:6b:b9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.98/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8d:6bb9/64 scope link
        valid_lft forever preferred_lft forever
```

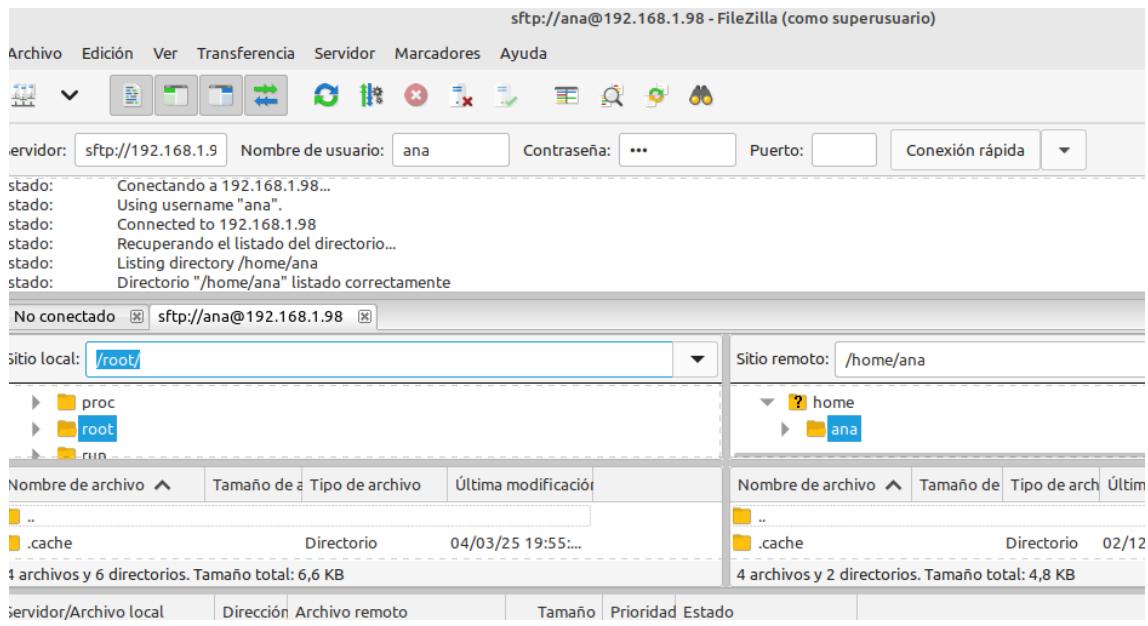
Usa el explorador de carpetas de los clientes linux y windows para acceder al servidor ssh.

Linux tenemos dos opciones

sftp://usuario@ip



La 2^a opción es mediante filezilla:



En Windows podemos usar filezilla o cualquier programa del estilo, por ejemplo, WinSCP.

Usa el comando scp para copiar ficheros a/desde el servidor ssh

Se haría de esta manera, pero primero debemos crear un documento.

```
[ -o SSH_OPTIONS [-i identity] [-S program] [source ...] target
usuario@clientelinux:~$ scp ana@192.168.1.98:/home/ana/ /home/usuario/
ana@192.168.1.98's password:
scp: /home/ana: not a regular file
usuario@clientelinux:~$
```

Ahora sí:

```
usuario@clientelinux:~$ scp ana@192.168.1.98:/home/ana/prueba.txt /home/usuario/
ana@192.168.1.98's password:
prueba.txt                                100%    8      7.9KB/s   00:00
```

Configura el servidor ssh para conectarse mediante certificado digital en lugar de usuario/password.

Primero vamos a generar las claves:

```
ana@192.168.1.98's password:  
prueba.txt  
usuario@clientelinux:~$ ssh-keygen -t rsa  
Generating public/private rsa key pair.  
Enter file in which to save the key (/home/usuario/.ssh/id_rsa):
```

Ahora copiaremos la clave pública al servidor:

```
usuario@clientelinux:~$ ssh-copy-id ana@192.168.1.98  
/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 prompt  
ed now it is to install the new keys  
ana@192.168.1.98's password:  
  
Number of key(s) added: 1  
  
Now try logging into the machine, with: "ssh 'ana@192.168.1.98'"  
and check to make sure that only the key(s) you wanted were added.
```

Ahora al conectarlos no nos debe pedir contraseña:

```
usuario@clientelinux:~$ ssh ana@192.168.1.98  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/pro  
  
System information as of mar 04 mar 2025 19:31:06 UTC  
  
System load: 0.0 Processes: 106  
Usage of /: 39.2% of 11.21GB Users logged in: 1  
Memory usage: 9% IPv4 address for enp0s3: 192.168.1.98  
Swap usage: 0%  
  
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»  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Mon Dec 2 19:39:12 2024 from 192.168.1.48  
ana@ana:~$
```

Crea túneles ssh para conectarte de manera segura a los distintos servicios del servidor

Para hacer con el puerto 8080:

```
usuario@clientelinux:~$ ssh -L 8080:localhost:80 ana@192.168.1.98
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

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

System information as of mar 04 mar 2025 19:34:31 UTC

System load: 0.0          Processes:           106
Usage of /: 39.2% of 11.21GB  Users logged in:    1
Memory usage: 9%          IPv4 address for enp0s3: 192.168.1.98
Swap usage:  0%

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»

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

Last login: Tue Mar  4 19:31:07 2025 from 192.168.1.99
ana@ana:~$
```

Para cualquier otro puerto será exactamente igual pero cambiando el puerto.