



SSH



¿Qué es SSH?

SSH (Secure Shell) es un protocolo de red seguro que sirve para **administrar sistemas de forma remota**. Su principal ventaja y la razón por la que sustituyó a protocolos más antiguos como Telnet es que

cifra todas las comunicaciones.

Las garantías que ofrece son:

- **Cifrado** de extremo a extremo.
- **Autenticación** de los usuarios que se conectan.
- **Integridad** de los datos para que no sean alterados durante la transmisión.

Seguridad y Configuración

Para asegurar un servidor SSH, la presentación recomienda las siguientes medidas:

- **Cambiar el puerto por defecto (22):** Este puerto es un objetivo común para atacantes, y cambiarlo reduce el riesgo de ataques automáticos.
- **Usar claves SSH en lugar de contraseñas:** Es un método de autenticación más seguro.
- **Deshabilitar el acceso del superusuario (root):** Se debe deshabilitar el root login para evitar que alguien obtenga control total del sistema de forma directa.
- **Activar un firewall:** Es fundamental para filtrar el tráfico y permitir únicamente las conexiones válidas al puerto SSH.
- **Monitorizar la actividad:** Se deben revisar los registros (logs) y vigilar los intentos de acceso fallidos.

El archivo principal para configurar el servidor se encuentra en

`/etc/ssh/sshd_config`.

Clientes para conectarse

La presentación menciona dos clientes principales para conectarse a un servidor SSH:

- **PuTTY:** Un cliente popular, gratuito y ligero para sistemas **Windows**.
- **Cliente OpenSSH en Ubuntu:** Se instala con el comando `sudo apt install openssh-client` y permite la conexión desde la terminal. Con el comando

ssh-copy-id se puede copiar fácilmente la clave pública al servidor para acceder sin necesidad de contraseña.

SSH

Actualizamos los repositorios y paquetes de nuestro sistema para tenerlo todo al día.

```
usuario@usuario:~$ sudo apt update && sudo apt upgrade
[sudo] contraseña para usuario:
0% [Esperando las cabeceras] [Esperando las cabeceras]
```

Instalamos del servidor OpenSSH.

```
usuario@usuario:~$ sudo apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  ncurses-term openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  molly-guard monkeysphere ssh-askpass
Se instalarán los siguientes paquetes NUEVOS:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 832 kB de archivos.
Se utilizarán 6.747 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
0% [Esperando las cabeceras]
```

Habilitamos el servicio SSH para que se inicie automáticamente con el sistema operativo.

```

usuario@usuario:~$ sudo systemctl status ssh
○ ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enab>
   Active: inactive (dead)
 TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
          man:sshd_config(5)
usuario@usuario:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/system
d/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.s
ervice.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/l
ib/systemd/system/ssh.service.
usuario@usuario:~$ sudo systemctl status ssh
○ ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>
   Active: inactive (dead)
 TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
          man:sshd_config(5)

```

Generamos un nuevo par de claves RSA de 4096 bits para la autenticación segura por SSH.

```

usuario@usuario:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.

Enter file in which to save the key (/home/usuario/.ssh/id_rsa): Enter passphras
e (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/usuario/.ssh/id_rsa
Your public key has been saved in /home/usuario/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:V9/dY8tRsZvPSg9lqpAc57H01DEESTzVXv/0d3k0anw usuario@usuario
The key's randomart image is:
+---[RSA 4096]---+
|           ooo.o |
|           +.  =|
|          ...o+ |
|         . o .O|
|        S o o +*B|
|       o = +oOB|
|      + = ** =|
|     = * E* |
|    = o = |
+-----[SHA256]-----+

```

Creamos una copia de seguridad del archivo de configuración del servidor SSH y procedemos a editarlo.

```

usuario@usuario:~$ sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.backup
usuario@usuario:~$ sudo nano /etc/ssh/sshd_config

```

Modificamos el archivo de configuración para cambiar el puerto de escucha por defecto del servicio SSH.

```
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:/usr/bin:/sbin:/bin

# 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 356
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key

^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich.^_ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea
```

```
GNU nano 7.2 /etc/ssh/sshd_config *

#Port 22
#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

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password

^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich.^_ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea
```

Deshabilitamos el inicio de sesión para el superusuario (root) por motivos de seguridad.

```
GNU nano 7.2 /etc/ssh/sshd_config *

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

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

#AuthorizedPrincipalsFile none

```

[^]G Ayuda [^]O Guardar [^]W Buscar [^]K Cortar [^]T Ejecutar [^]C Ubicación
[^]X Salir [^]R Leer fich. [^]\ Reemplazar [^]U Pegar [^]J Justificar [^]/ Ir a línea

```
GNU nano 7.2 /etc/ssh/sshd_config *

# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options

```

[^]G Ayuda [^]O Guardar [^]W Buscar [^]K Cortar [^]T Ejecutar [^]C Ubicación
[^]X Salir [^]R Leer fich. [^]\ Reemplazar [^]U Pegar [^]J Justificar [^]/ Ir a línea

```
usuario@usuario: ~
GNU nano 7.2 /etc/ssh/sshd_config *
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
ClientAliveInterval 300
ClientAliveCountMax 2
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

^G Ayuda      ^O Guardar   ^W Buscar    ^K Cortar    ^T Ejecutar  ^C Ubicación
^X Salir      ^R Leer fich.^_ Reemplazar ^U Pegar     ^J Justificar^/ Ir a línea
```

```
usuario@usuario: ~
GNU nano 7.2 /etc/ssh/sshd_config *
#RekeyLimit default none

# Logging
SyslogFacility AUTH
LogLevel VERBOSE

# Authentication:

LoginGraceTime 2m
PermitRootLogin no
StrictModes no
MaxAuthTries 6
MaxSessions 10

PubkeyAuthentication yes

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

#AuthorizedPrincipalsFile none

^G Ayuda      ^O Guardar   ^W Buscar    ^K Cortar    ^T Ejecutar  ^C Ubicación
^X Salir      ^R Leer fich.^_ Reemplazar ^U Pegar     ^J Justificar^/ Ir a línea
```

```
usuario@usuario: ~  
GNU nano 7.2 /etc/ssh/sshd_config *  
# Expect .ssh/authorized_keys2 to be disregarded by default in future.  
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2  
  
#AuthorizedPrincipalsFile none  
  
#AuthorizedKeysCommand none  
#AuthorizedKeysCommandUser nobody  
  
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts  
#HostbasedAuthentication no  
# Change to yes if you don't trust ~/.ssh/known_hosts for  
# HostbasedAuthentication  
#IgnoreUserKnownHosts no  
# Don't read the user's ~/.rhosts and ~/.shosts files  
#IgnoreRhosts yes  
  
# To disable tunneled clear text passwords, change to no here!  
PasswordAuthentication yes  
#PermitEmptyPasswords no
```

Reiniciamos el servicio SSH para aplicar los cambios de configuración.

```
usuario@usuario:~$ sudo systemctl restart ssh
```

Configuramos las interfaces de red para establecer una dirección IP estática en una de ellas.

```
GNU nano 7.2 /etc/netplan/01-netcfg.yaml *
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: yes
    enp0s8:
      dhcp4: no
      addresses:
        - 192.168.1.10/24
      gateway4: 192.168.1.10

^G Ayuda      ^O Guardar   ^W Buscar    ^K Cortar    ^T Ejecutar  ^C Ubicación
^X Salir      ^R Leer fich.^\\ Reemplazar ^U Pegar     ^J Justificar^/_ Ir a línea
```

Aplicamos la configuración de red que acabamos de modificar.

```
usuario@usuario:~$ sudo netplan apply

** (generate:4192): WARNING **: 12:33:09.043: `gateway4` has been deprecated, use
e default routes instead.
See the 'Default routes' section of the documentation for more details.

** (generate:4192): WARNING **: 12:33:09.044: Permissions for /etc/netplan/01-ne
twork-manager-all.yaml are too open. Netplan configuration should NOT be accessi
ble by others.

** (process:4190): WARNING **: 12:33:09.852: `gateway4` has been deprecated, use
e default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:4190): WARNING **: 12:33:09.853: Permissions for /etc/netplan/01-net
work-manager-all.yaml are too open. Netplan configuration should NOT be accessib
le by others.

** (process:4190): WARNING **: 12:33:10.027: `gateway4` has been deprecated, use
e default routes instead.
See the 'Default routes' section of the documentation for more details.
```

Consultamos el estado del cortafuegos y permitimos el tráfico SSH.

```
usuario@usuario:~$ sudo ufw status
Estado: inactivo
usuario@usuario:~$ sudo ufw allow ssh
Reglas actualizadas
Reglas actualizadas (v6)
```

Abrimos el puerto 365 con el protocolo TCP para permitir el acceso.

```
usuario@usuario:~$ sudo ufw allow 365/tcp
Reglas actualizadas
Reglas actualizadas (v6)
```

Cliente:

Estamos editando la configuración de red del cliente para asignarle una dirección IP estática.

```
GNU nano 7.2 /etc/netplan/01-netcfg.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s8:
      dhcp4: yes
    enp0s8:
      dhcp4: no
      addresses:
        - 192.168.1.20/24
      gateway4: 192.168.1.10
```

[11 líneas escritas]

^G Ayuda	^O Guardar	^W Buscar	^K Cortar	^T Ejecutar	^C Ubicación
^X Salir	^R Leer fich.	^_ Reemplazar	^U Pegar	^J Justificar	^_ Ir a línea

Aplicamos la configuración de red que acabamos de modificar.

```
usuario@usuario:~$ sudo netplan apply

** (generate:4192): WARNING **: 12:33:09.043: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (generate:4192): WARNING **: 12:33:09.044: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.

** (process:4190): WARNING **: 12:33:09.852: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:4190): WARNING **: 12:33:09.853: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.

** (process:4190): WARNING **: 12:33:10.027: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.
```

Instalamos el cliente OpenSSH para poder establecer una conexión remota con el servidor.

```
usuario@usuario:~$ sudo apt install openssh-client -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
openssh-client ya está en su versión más reciente (1:9.6p1-3ubuntu13.5).
fijado openssh-client como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
usuario@usuario:~$
```

Nos conectamos remotamente al servidor a través de SSH con el cliente.

```
usuario@usuario:~$ ssh-copy-id -p 356 usuario@192.168.1.10
/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
usuario@192.168.1.10's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -p 356 'usuario@192.168.1.10'"
and check to make sure that only the key(s) you wanted were added.

usuario@usuario:~$ ssh usuario@192.168.1.10 -p 356
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.14.0-32-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»
```

EXTENSIÓN (Nombre de Dominio):

Vamos a editar el archivo hosts para asociar direcciones IP con nombres de dominio.

```
usuario@usuario:~$ sudo nano /etc/hosts
[sudo] contraseña para usuario:
```

Añadimos la dirección IP del servidor y le asignamos un nombre de dominio para poder referirnos a él de forma más sencilla.

```
GNU nano 7.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 usuario
192.168.1.10 miservidor

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea

Utilizamos el alias creado para conectarnos al servidor de manera más sencilla.

```
usuario@usuario:~$ ssh usuario@miservidor -p 356
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.14.0-32-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»

Last login: Wed Oct  1 13:19:59 2025 from 192.168.1.20
```