

Configuración del servidor OpenSSH en “servidor- planetas”

Generación de claves

En primer lugar, generaré un par de llaves de cifrado asimétrico para utilizarlas como método de autenticación en el servidor. Generaré el par de llaves en el equipo administrador para copiar la clave publica en “servidor-planetas” mediante el comando:

```
ssh-keygen -t rsa -b 4096 -C "servidor-planetas" -f /var/root/.ssh/servidor-planetas
```

Y mediante este comando se generaron en el directorio /var/root/.ssh/ del equipo administrador las claves:

```
sh-3.2# ls /var/root/.ssh/  
servidor-planetas      servidor-planetas.pub
```

Ahora procederemos a enviar la clave publica a “servidor-planetas” mediante el comando:

ssh-copy-id -i ~/.ssh/servidor-planetas.pub admin-servidor@192.168.1.129

```
sh-3.2# ssh-copy-id -i ~/.ssh/servidor-planetas.pub admin-servidor@192.168.1.129
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/var/root/.ssh/servidor-planetas.pub"
The authenticity of host '192.168.1.129 (192.168.1.129)' can't be established.
ED25519 key fingerprint is SHA256:9JymGdEd+hIYpyv5U7wSYu003ajU6FILPAj29SjtJeo.
This key is not known by any other names.
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 prompted now it is to install the new keys
admin-servidor@192.168.1.129's password:

Number of key(s) added:      1

Now try logging into the machine, with:  "ssh 'admin-servidor@192.168.1.129'"
and check to make sure that only the key(s) you wanted were added.
```

Modificación de archivo de configuración

Ahora al intentar iniciar sesión nos sigue pidiendo la contraseña, procedemos a deshabilitar el acceso mediante el uso de contraseña modificando el archivo de configuración del servidor OpenSSH en la ruta de “servidor-planetas”: “/etc/ssh/sshd_config” y deshabilitamos las opciones:

PasswordAuthentication no

PermitRootLogin no

Y habilitamos la opción

PubkeyAuthentication yes

```
# 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
# 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 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 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

#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 no
PermitEmptyPasswords no
```

Pruebas de conectividad

Gracias a esto ahora podemos acceder a “servidor-planetas” directamente sin utilizar contraseña desde el equipo administrador mediante el siguiente comando:

```
ssh -i /var/root/.ssh/servidor-planetas admin-servidor@192.168.1.129
```

```
[sh-3.2# ssh -i ~/.ssh/servidor-planetas admin-servidor@192.168.1.129
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-55-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Mar 23 15:48:56 2025 from 192.168.1.187
```

Si intentamos iniciar sesión de manera normal sin especificar la ruta de la clave nos negará el acceso ya que hemos deshabilitado la autenticación por contraseña:

```
[sh-3.2# ssh admin-servidor@192.168.1.129
admin-servidor@192.168.1.129: Permission denied (publickey).
```