Configuración del servidor OpenSSH en “raspberrypi”

Instalación de OpenSSH

Instalamos el servidor ssh mediante el comando:

·sudo apt install openssh-server

Generación de claves

En primer lugar, generaré un par de llaves de cifrado asimétrico para utilizarlas como método de autenticación en la raspberry. 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 "raspberry" -f /var/root/.ssh/raspberry

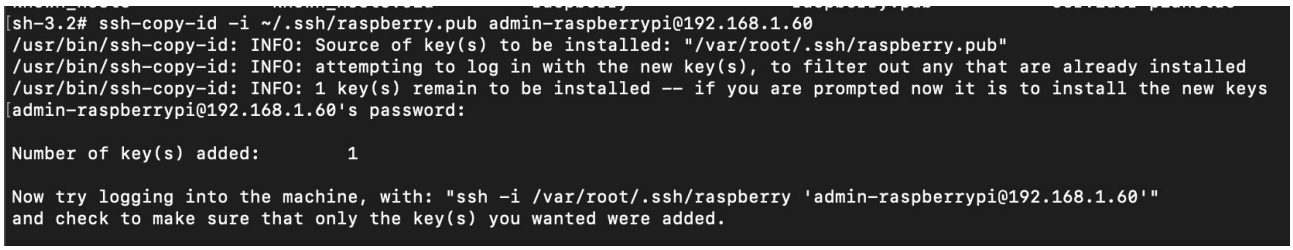
```
sh-3.2# ssh-keygen -t rsa -b 4096 -C "raspberry" -f /var/root/.ssh/raspberry
Generating public/private rsa key pair.
Enter passphrase for "/var/root/.ssh/raspberry" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /var/root/.ssh/raspberry
Your public key has been saved in /var/root/.ssh/raspberry.pub
The key fingerprint is:
SHA256:zRYAcm17hsilqvMSH23C+z8E15cvt9h7iX47K7xgJEk raspberry
The key's randomart image is:
+---[RSA 4096]----+
|     . oo.       |
|      o  +.      |
|     . = E.  .   |
|      = =o=.o    |
|   . o oS=+o .   |
|  . = o ..o . o  |
|   + = .   o.=...|
|  + o   . . o+o+.|
|   +.....  .o==+|
+----[SHA256]-----+
```

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

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

Ahora procederemos a enviar la clave publica a “raspberrypi” mediante el comando:

ssh-copy-id -i ~/.ssh/raspberry.pub admin-raspberrypi@192.168.1.60



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 “raspberry”: “/etc/ssh/sshd_config” y deshabilitamos las opciones:

PasswordAuthentication no

PermitRootLogin no

Y habilitamos la opción

PubkeyAuthentication yes

```
  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:/us

# 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 siguente comando:

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

```
[sh-3.2# ssh -i ~/.ssh/raspberry admin-raspberrypi@192.168.1.60
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1028-raspi aarch64)

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

 System information as of Sat May 24 21:31:09 CEST 2025

  System load:           0.0
  Usage of /:            4.1% of 57.99GB
  Memory usage:          3%
  Swap usage:            0%
  Temperature:           41.9 C
  Processes:             159
  Users logged in:       1
  IPv4 address for eth0: 192.168.1.60
  IPv6 address for eth0: 2a0c:5a80:d30f:8f00:dea6:32ff:fed7:3322

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Sat May 24 21:31:11 2025 from 192.168.1.209
admin-raspberrypi@raspberrypi:~$
```

Si intentamos iniciar sesion 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-raspberrypi@192.168.1.60
admin-raspberrypi@192.168.1.60: Permission denied (publickey).
```

El servidor SSH queda instalado y configurado en la raspberry