

SSH sin Password:

En este trabajo, tendremos que conseguir que el PC1 se conecte al PC2 sin tener que poner la contraseña. Para realizarlo haremos lo siguiente:

- 1) Lo primero que tenemos que hacer es activar el servicio de SSH en ambos PCs. Ponemos el siguiente comando:
 - ✓ `$ sudo service ssh start`
- 2) Para comprobar que está encendido:
 - ✓ `$ service ssh status`

```
usuario@usuario-ALDA: ~
usuario@usuario-ALDA:~$ sudo service ssh start
[sudo] password for usuario:
usuario@usuario-ALDA:~$ service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since lun 2019-02-25 08:19:53 CET; 11min ago
     Process: 4844 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCE
     Process: 4843 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
     Process: 1781 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 2067 (sshd)
      Tasks: 1
     Memory: 3.2M
        CPU: 37ms
    CGroup: /system.slice/ssh.service
            └─2067 /usr/sbin/sshd -D

feb 25 08:21:37 usuario-ALDA sshd[2067]: Server listening on 0.0.0.0 port 22.
feb 25 08:21:37 usuario-ALDA sshd[2067]: Server listening on :: port 22.
feb 25 08:21:37 usuario-ALDA systemd[1]: Reloading OpenBSD Secure Shell server.
feb 25 08:21:37 usuario-ALDA sshd[2067]: Received SIGHUP; restarting.
feb 25 08:21:37 usuario-ALDA sshd[2067]: Server listening on 0.0.0.0 port 22.
feb 25 08:21:37 usuario-ALDA sshd[2067]: Server listening on :: port 22.
feb 25 08:21:37 usuario-ALDA systemd[1]: Reloaded OpenBSD Secure Shell server.
feb 25 08:30:44 usuario-ALDA systemd[1]: Started OpenBSD Secure Shell server.
```

- 3) Después creamos la contraseña aleatoria para que nos podamos conectar al PC2 sin tener que poner la contraseña con el siguiente comando:

`$ ssh-keygen -b 4096 -t rsa`

- ✓ Al poner el comando, le damos a enter tres veces y nos saldrá lo siguiente:

```
usuario@usuario-ALDA: ~
feb 25 08:31:09 usuario-ALDA systemd[1]: Started OpenBSD Secure Shell server.

usuario@usuario-ALDA:~$ ssh-keygen -b 4096 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/usuario/.ssh/id_rsa):
Enter passphrase (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:Q5LY7KS+0Px847IWzr743E2hLCnL/DHv7fju0TBwqmI usuario@usuario-ALDA
The key's randomart image is:
+----[RSA 4096]-----+
|
|  + .
|  . * .
|  +.o.
| o ++S
| B.=.ooo
| ooXoB .o
| E=O B o..
| ..B.+.=B.
+----[SHA256]-----+
usuario@usuario-ALDA:~$
```

- 4) Tras generar la contraseña publica, tenemos que enviársela al PC2 para que nos deje entrar en su ordenador sin tener que poner su contraseña.

```
$ sudo ssh-copy-id usuario@192.168.42.1
```

- ✓ En el nombre de usuario le tenemos que poner el nombre del usuario en el que queremos entrar, y tiene que existir en el PC2, y la IP tenemos que poner la IP del PC2.

```
usuario@usuario-ALDA:~$ sudo ssh-copy-id usuario@192.168.42.1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/usuario/.ssh/id_rsa.pub"
The authenticity of host '192.168.42.1 (192.168.42.1)' can't be established.
ECDSA key fingerprint is SHA256:JpeJYryqi7Ig94dn+e0hKLS0eJ1EuVIRh5oFb6WaiR0.
Are you sure you want to continue connecting (yes/no)? 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 prompt
ed now it is to install the new keys
usuario@192.168.42.1's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'usuario@192.168.42.1'"
and check to make sure that only the key(s) you wanted were added.

usuario@usuario-ALDA:~$
```

Nos pedirá la contraseña del usuario y después de esto, solo tendríamos que conectar con el comando:

```
$ ssh usuario@192.168.42.1
```

y no nos volverá a pedir contraseña para volver a conectarnos.

```
usuario@usuario-ALDA:~$ ssh usuario@192.168.42.1
The authenticity of host '192.168.42.1 (192.168.42.1)' can't be established.
ECDSA key fingerprint is SHA256:JpeJYryqi7Ig94dn+e0hKLS0eJ1EuVIRh5oFb6WaiR0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.42.1' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.1 x86_64)

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

113 packages can be updated.
23 updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Feb 25 08:36:22 2019 from 192.168.11.65
usuario@usuario-ALDA:~$ s
```