

# SERVIDOR SHH CON CLAVES PUBLICA Y PRIVADA

Autor : Pablo Horcajada González

Profesor : Guillermo Bellettini

Fecha : 28/09/2021

Clase : Despliegue Web

## Contenido

Instalación SHH en ambas maquinas .....	2
Instalamos el servicio de ssh en Ubuntu .....	2
Instalamos el servidor OpenSSH en CentOS.....	2
Configuración servidor SSH .....	2
Hacemos una copia del archivo original.....	2
Modificamos el archivo cambiando el puerto y los permisos de root .....	2
Reiniciamos el servidor.....	2
Configuración del Firewall.....	3
Abrimos el puerto que hemos cambiado .....	3
Reiniciamos el Firewall(en caso de ser el servidor CentOS).....	3
Vemos la dirección ip de la maquina servidor .....	3
Nos conectamos al servidor Ubuntu desde CentOS (usuario ubu) .....	3
Configuración Claves y Envío.....	4
Creamos el par de claves.....	4
Guardamos el par de claves en el subdirectorio .ssh/ .....	4
Introducimos una frase/palabra de contraseña para dicho archivo .....	4
Guardamos la clave publica en un fichero .....	4
Enviamos el archivo con la clave pública desde el servidor al cliente (con scp) .....	4
Enviamos el archivo con la clave pública desde el servidor al cliente (con ssh) .....	4
Comprobamos que he llegado en el cliente.....	5

# Instalación SSH en ambas maquinas

Instalamos el servicio de ssh en Ubuntu

```
root@ubu-VirtualBox:~# apt-get install openssh-server openssh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-client is already the newest version (1:8.2p1-4ubuntu0.4).
```

Instalamos el servidor OpenSSH en CentOS

```
[pablo@CTSPHG ~]$ yum install openssh-server
Error: Este comando debe ejecutarse con privilegios de superusuario (bajo el usuario root en la mayoría de los sistemas).
[pablo@CTSPHG ~]$ sudo yum install openssh-server

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for pablo:
CentOS Linux 8 - AppStream          6.7 MB/s | 9.2 MB      00:01
CentOS Linux 8 - BaseOS             12 MB/s | 7.5 MB      00:00
CentOS Linux 8 - Extras             29 kB/s | 12 kB       00:00
El paquete openssh-server-8.0p1-6.el8_4.2.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
```

## Configuración servidor SSH

Hacemos una copia del archivo original

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.old
```

Modificamos el archivo cambiando el puerto y los permisos de root

```
#Port 2244
```

```
#PermitRootLogin yes
```

Reiniciamos el servidor

```
sudo systemctl reload sshd
```

# Configuración del Firewall

Abrimos el puerto que hemos cambiado

-Versión CentOS

```
[pablo@CTSPHG ~]$ sudo firewall-cmd --permanent --add-port=2244/tcp
success
```

-Versión Ubuntu

```
ubu@ubu-VirtualBox:~$ sudo ufw allow 2244/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
```

Reiniciamos el Firewall(en caso de ser el servidor CentOS)

```
[pablo@CTSPHG ~]$ sudo firewall-cmd --reload
success
[pablo@CTSPHG ~]$
```

Vemos la dirección ip de la maquina servidor

```
ubu@ubu-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.31.237.253 netmask 255.255.240.0 broadcast 172.31.239.255
    inet6 fe80::68d:5fc0:5378:d3a9 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:fa:72:b1 txqueuelen 1000 (Ethernet)
    RX packets 110063 bytes 158745639 (158.7 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2911 bytes 264917 (264.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 265 bytes 23864 (23.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 265 bytes 23864 (23.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Nos conectamos al servidor Ubuntu desde CentOS (usuario ubu)

```
[Pablo@CTSPHG pablo]$ ssh ubu@172.31.237.253
ubu@172.31.237.253's password:
Welcome to Ubuntu 20.10 (GNU/Linux 5.8.0-63-generic x86_64)

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

0 updates can be installed immediately.
0 of these updates are security updates.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '21.04' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep 28 16:07:09 2021 from 172.31.233.179
ubu@ubu-VirtualBox:~$
```

# Configuración Claves y Envió

Creamos el par de claves

```
ubu@ubu-VirtualBox:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ubu/.ssh/id_rsa):
```

Guardamos el par de claves en el subdirectorio .ssh/

```
Enter file in which to save the key (/home/ubu/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
```

Introducimos una frase/palabra de contraseña para dicho archivo

-En mi caso pongo "pablo". Al escribirla no se muestra por pantalla

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ubu/.ssh/id_rsa
Your public key has been saved in /home/ubu/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:XLNvjemUCyKZNxVvBFb960yfkB87bkgufBUru4UUsto ubu@ubu-VirtualBox
The key's randomart image is:
+---[RSA 3072]-----+
|
|      =+O. |
|      o o  |
|      . =. .O..|
|      . = 0.O..|
|      S +..+ o |
|      .oo.B=O |
|      ..EX=*o |
|      * *=O+ |
|      +. +*O |
|
+----[SHA256]-----+
ubu@ubu-VirtualBox:~$ cp /home/ubu/.ssh/id_rsa.pub >> /home/ubu/clave_publica
```

Guardamos la clave publica en un fichero

```
cat /home/ubu/.ssh/id_rsa.pub >> /home/ubu/clave_publica
```

Enviamos el archivo con la clave pública desde el servidor al cliente (con scp)

```
ubu@ubu-VirtualBox:~$ sudo scp /home/ubu/clave_publica Pablo@172.31.233.179:/home/pablo/clave
Pablo@172.31.233.179's password:
clave_publica 100% 572 114.4KB/s 00:00
```

Enviamos el archivo con la clave pública desde el servidor al cliente (con ssh)

```
root@ubu-VirtualBox:~/.ssh# ssh-copy-id -i id_rsa.pub Pablo@172.19.93.5
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are a
lready installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to in
stall the new keys
Pablo@172.19.93.5's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'Pablo@172.19.93.5'"
and check to make sure that only the key(s) you wanted were added.
```

## Comprobamos que he llegado en el cliente

```
[Pablo@CTSPHG pablo]$ ls
clave  clave_publica
[Pablo@CTSPHG pablo]$ pwd
/home/pablo
[Pablo@CTSPHG pablo]$ cat clave
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDQqkLanw40cUyTEkXbhzPG83Us7k3B1ByiLC37L1rDwwLNæu/4pbL00RuxUew
ImoMJmf t?sIvMnDTGJEB+wi+3110XbBm1m1T+pFAbf03gIMDFCtp6UkLY6nSsr0fABiUQNxcAyLfLnzWoPBd+vqg3zi2kL3YoYrD
GuM70hdqP/pdZ4gg15sQ4beu9KkkxDuCa4KGGCzT+ABDVNgofykDZ+0uxXwZ491U91Bmcvj/4P+oCJ258tug/+DfqxLF8YuNhTMF
Yd/3HgacQOFc4wdTBSB84rR6tiAe3uTML0CexQWjvmsZQCa/Ion01F6yxsnale+8luHASmu7BSqZ/3M3UqwtNstSp/1jeABtA04f
ogZYKZT8ven9SSNIMsJLymIeKlqC5UGrYQm8EgCvn9YGE84skqSutU0qji tNEGszzrTzy6+o9/kkkuKOLJ3lqq/wæAeGnYZfs14DU
bZwgG0yWZqZf7mLbctco0A53PqDFdHpntMGUf55nIf/Dan1057M= ubu@ubu-VirtualBox
```