

Acceso SSH

03/10/2023

Guillermo Bellettini

Seguridad

Creado por: Nicolas Pavel Ballesteros Barrado



Contenido

Acceso SSH	1
Arrancamos las dos maquinas.....	3
Las maquinas se hacen ping entre ellas.....	3
Nos vamos a la carpeta .ssh	4
Ponemos el comando ll.....	4
Comando more known_host.....	4
Nos conectamos remotamente al usuario.....	5
Ponemos su IP para podernos conectar	5
Ponemos el comando ssh usuario@10.68.16.56	5
Ponemos el comando pwd	6
Ponemos el comando ssh-keygen	6
Ponemos otra vez el comando ll	6
Ponemos comando ssh-copy-id -i.....	7
Nos conectamos ahora sin que nos pida contraseña	7
Comando More authorized_keys	8

Arrancamos las dos maquinas



LUBUNTU_Guillermo

➡ Corriendo



LUBUNTU_Seguridad

➡ Corriendo

Las maquinas se hacen ping entre ellas

```
1/1 + Tili: Por defecto
1:root@ubuntu: ~
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 (Bucle local)
    RX packets 59 bytes 7106 (7.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 59 bytes 7106 (7.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:~# ping 10.68.16.60
PING 10.68.16.60 (10.68.16.60) 56(84) bytes of data.
64 bytes from 10.68.16.60: icmp_seq=1 ttl=64 time=0.361 ms
64 bytes from 10.68.16.60: icmp_seq=2 ttl=64 time=0.906 ms
64 bytes from 10.68.16.60: icmp_seq=3 ttl=64 time=0.855 ms
64 bytes from 10.68.16.60: icmp_seq=4 ttl=64 time=0.816 ms
64 bytes from 10.68.16.60: icmp_seq=5 ttl=64 time=0.690 ms
64 bytes from 10.68.16.60: icmp_seq=6 ttl=64 time=0.712 ms
64 bytes from 10.68.16.60: icmp_seq=7 ttl=64 time=0.755 ms
64 bytes from 10.68.16.60: icmp_seq=8 ttl=64 time=0.972 ms
64 bytes from 10.68.16.60: icmp_seq=9 ttl=64 time=1.03 ms
64 bytes from 10.68.16.60: icmp_seq=10 ttl=64 time=0.512 ms
64 bytes from 10.68.16.60: icmp_seq=11 ttl=64 time=0.734 ms

64 bytes from 10.68.16.56: icmp_seq=17 ttl=64 time=0.937 ms
64 bytes from 10.68.16.56: icmp_seq=18 ttl=64 time=0.731 ms
64 bytes from 10.68.16.56: icmp_seq=19 ttl=64 time=0.703 ms
64 bytes from 10.68.16.56: icmp_seq=20 ttl=64 time=0.947 ms
64 bytes from 10.68.16.56: icmp_seq=21 ttl=64 time=0.931 ms
64 bytes from 10.68.16.56: icmp_seq=22 ttl=64 time=0.673 ms
64 bytes from 10.68.16.56: icmp_seq=23 ttl=64 time=0.699 ms
64 bytes from 10.68.16.56: icmp_seq=24 ttl=64 time=0.856 ms
64 bytes from 10.68.16.56: icmp_seq=25 ttl=64 time=0.825 ms
64 bytes from 10.68.16.56: icmp_seq=26 ttl=64 time=0.640 ms
64 bytes from 10.68.16.56: icmp_seq=27 ttl=64 time=0.963 ms
64 bytes from 10.68.16.56: icmp_seq=28 ttl=64 time=0.779 ms
64 bytes from 10.68.16.56: icmp_seq=29 ttl=64 time=0.774 ms
64 bytes from 10.68.16.56: icmp_seq=30 ttl=64 time=0.434 ms
64 bytes from 10.68.16.56: icmp_seq=31 ttl=64 time=0.871 ms
64 bytes from 10.68.16.56: icmp_seq=32 ttl=64 time=0.802 ms
64 bytes from 10.68.16.56: icmp_seq=33 ttl=64 time=0.186 ms
64 bytes from 10.68.16.56: icmp_seq=34 ttl=64 time=0.186 ms
64 bytes from 10.68.16.56: icmp_seq=35 ttl=64 time=0.939 ms
64 bytes from 10.68.16.56: icmp_seq=36 ttl=64 time=0.814 ms
64 bytes from 10.68.16.56: icmp_seq=37 ttl=64 time=0.248 ms
64 bytes from 10.68.16.56: icmp_seq=38 ttl=64 time=1.04 ms
64 bytes from 10.68.16.56: icmp_seq=39 ttl=64 time=0.918 ms
64 bytes from 10.68.16.56: icmp_seq=40 ttl=64 time=0.510 ms
64 bytes from 10.68.16.56: icmp_seq=41 ttl=64 time=0.638 ms
64 bytes from 10.68.16.56: icmp_seq=42 ttl=64 time=0.974 ms
64 bytes from 10.68.16.56: icmp_seq=43 ttl=64 time=0.635 ms
64 bytes from 10.68.16.56: icmp_seq=44 ttl=64 time=0.791 ms
64 bytes from 10.68.16.56: icmp_seq=45 ttl=64 time=0.804 ms
64 bytes from 10.68.16.56: icmp_seq=46 ttl=64 time=0.410 ms
64 bytes from 10.68.16.56: icmp_seq=47 ttl=64 time=0.740 ms
64 bytes from 10.68.16.56: icmp_seq=48 ttl=64 time=0.634 ms
64 bytes from 10.68.16.56: icmp_seq=49 ttl=64 time=0.430 ms
64 bytes from 10.68.16.56: icmp_seq=50 ttl=64 time=0.956 ms
64 bytes from 10.68.16.56: icmp_seq=51 ttl=64 time=0.346 ms
64 bytes from 10.68.16.56: icmp_seq=52 ttl=64 time=0.331 ms
```

Nos vamos a la carpeta .ssh

```
root@npa:~# cd .ssh
root@npa:~/ssh# _
```

Esta carpeta si existe ya que estamos en un Ubuntu server

Ponemos el comando ll

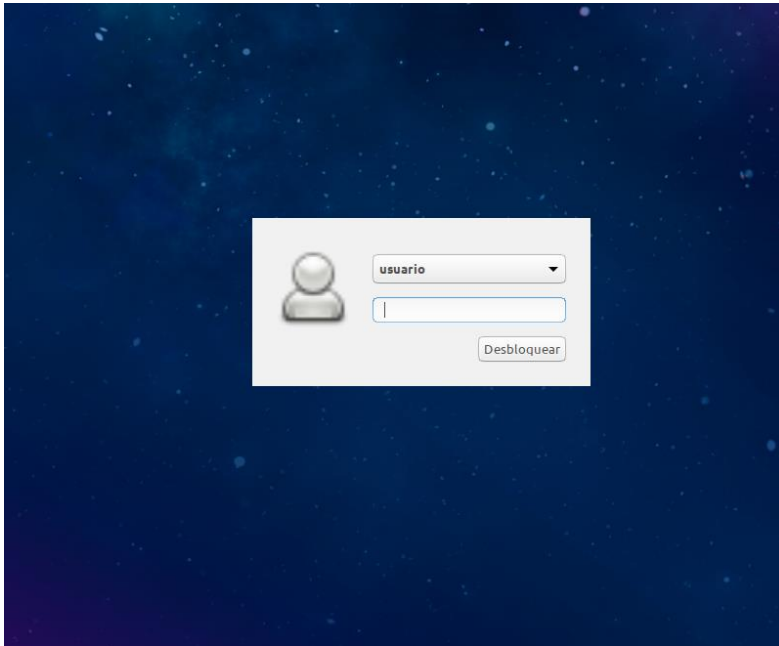
```
root@npa:~# ll
total 24
drwx----- 4 root root 4096 sep 29 18:49 ./
drwxr-xr-x 19 root root 4096 sep 29 18:35 ../
-rw-r--r-- 1 root root 3106 oct 15 2021 .bashrc
-rw-r--r-- 1 root root 161 jul 9 2019 .profile
drwx----- 3 root root 4096 sep 29 18:49 snap/
drwx----- 2 root root 4096 sep 29 18:49 .ssh/
root@npa:~# _
```

Comando more known_host

```
root@npa:~# more known_host
more: cannot open known_host: No such file or directory
root@npa:~# more known_hosts
more: cannot open known_hosts: No such file or directory
root@npa:~#
```

Se genera este fichero cuando te conectas con control remoto al servidor, en este caso no existe ya que no estoy conectado y nadie ha sido conectado por control remoto

Nos conectamos remotamente al usuario



Ponemos su IP para podernos conectar

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.68.16.56 netmask 255.255.252.0 broadcast 10.68.19.255
    inet6 fe80::a00:27ff:febb:2dbc prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:bb:2d:bc txqueuelen 1000 (Ethernet)
    RX packets 36951 bytes 3807414 (3.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 673 bytes 58355 (58.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ponemos el comando ssh usuario@10.68.16.56

```
root@npa:~# ssh usuario@10.68.16.56
The authenticity of host '10.68.16.56 (10.68.16.56)' can't be established.
ED25519 key fingerprint is SHA256:qKB5uZFXTE/KDQSpAKoE0ngN2c56un7S3P8b5CjAKLA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.68.16.56' (ED25519) to the list of known hosts.
usuario@10.68.16.56's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 399 paquetes.
326 actualizaciones son de seguridad.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

usuario@ubuntu:~$ _
```

Ya estamos conectado

Ponemos el comando pwd

```
usuario@ubuntu:~$ pwd
/home/usuario
usuario@ubuntu:~$ _
```

Ponemos el comando ssh-keygen

```
root@npa:~/.ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:xs5QvuAgFV2A9jrJ3zX8irmPWatNvhFYSSheFIkrTWQ root@npa
The key's randomart image is:
+---[RSA 3072]-----+
|      .+E++0      |
|      0++0.      |
|     ..+0.+ .    |
|     ...+* +     |
|     ...++ S..   |
|     . = 0 * .+. |
|      0..+..+0   |
|      . .X 0.    |
|      B+B0       |
+---[SHA256]-----+
root@npa:~/.ssh#
```

Ponemos otra vez el comando ll

```
root@npa:~/.ssh# ll
total 24
drwx----- 2 root root 4096 oct  3 16:50 ./
drwx----- 4 root root 4096 oct  3 16:49 ../
-rw----- 1 root root   0 sep 29 18:49 authorized_keys
-rw----- 1 root root 2590 oct  3 16:50 id_rsa
-rw-r--r-- 1 root root  562 oct  3 16:50 id_rsa.pub
-rw----- 1 root root  364 oct  3 16:32 known_hosts
-rw-r--r-- 1 root root  142 oct  3 16:32 known_hosts.old
root@npa:~/.ssh#
```

Ponemos comando ssh-copy-id -i

```
pavel@npa:~/ssh$ ssh-copy-id -i /home/pavel/.ssh/id_rsa.pub usuario@10.68.16.56
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/pavel/.ssh/id_rsa.pub"
The authenticity of host '10.68.16.56 (10.68.16.56)' can't be established.
ED25519 key fingerprint is SHA256:oKB5uZFXTE/KDQSpAKoEOngN2c56un7S3P8b5CjAKLA.
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 all the new keys
usuario@10.68.16.56's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'usuario@10.68.16.56'"
and check to make sure that only the key(s) you wanted were added.

pavel@npa:~/ssh$
```

Ya nos dicen que ya se ha añadido en el servidor remoto

Nos conectamos ahora sin que nos pida contraseña

```
pavel@npa:~/ssh$ ssh usuario@10.68.16.56
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 399 paquetes.
326 actualizaciones son de seguridad.

Last login: Tue Oct  3 18:34:44 2023 from 10.68.16.60
usuario@ubuntu:~$ _
```

Nos deja acceder porque hemos copiado la clave publica al servidor destino

Nos vamos conectados a la carpeta .ssh y ejecutamos el comando ll nos sale una carpeta llamada llaves autorizadas y que tienen las claves permitidas para conectarnos al servidor

```
usuario@ubuntu:~/ssh$ ll
total 12
drwx----- 2 usuario usuario 4096 oct  3 19:06 ./
drwxr-xr-x 18 usuario usuario 4096 oct  3 19:06 ../
-rw----- 1 usuario usuario  563 oct  3 19:06 authorized_keys
usuario@ubuntu:~/ssh$
```

Comando More authorized_keys

```
usuario@ubuntu:~/ssh$ more authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDP5YUFkcbgoMETwb0ZeurMsbq7pfUndbt00F5sNFTPvwGEvH5adgMYGJ3m71+G
UOPv4oDjebwuy61tbEwuxyGczTMeFA9+bq16tnEj/koy5NLbg22Pi0XGCIIQLauXUWW7VfK1kBS9nH2/1hzQSmX3cNDdyhtG9PuX
/XwYHKroQ/r870KcCVT++McudHgKTR788bGNw3fvf5nMI1L3kQpmBEAaPGs0AkS00zt71NPtAh5ze9UwvT4BsxKgg1Hc0rxmHUNf
N2w1b0sPzGxsUsIqg7L7tNDs9doPrBU5Rtk00vZibmUCr7opxYhVoP//7wuBPXoXg0E8vL2SEPixLfIv0SLsqGGE/2c9VBejYUHT
QBg/tUBE4D852iIhNxFvCoxq5wN1dCD9CTOMMNkDz9yqsNDzRMteX39QMhiejFkpR0iy1E/DjUFECia0Psfj0p+z8e1KLXK18ZGk
gEuhSPE9XU/BKNH0QCeKva8wkeaW3Aw4tH5FVadtNCpqn80f++E= pavel@npa
usuario@ubuntu:~/ssh$ _
```

Nos sale la clave encriptada y si leemos al final nos pone el nombre del usuario pavel@npa, es el que genero las claves.