



Práctica 5 - SSH

Preparativos

Crear un grupo y los usuarios

Gestionar los permisos

Fichero principal de configuración

Carpeta raíz y de usuarios

Comprobación

Preparativos

Crear un grupo y los usuarios

```
chell@aperturelaboratories: ~  
chell@aperturelaboratories:~$ sudo group  
groupadd groupdel groupmems groupmod groups  
chell@aperturelaboratories:~$ sudo groupadd practica5  
[sudo] password for chell:  
chell@aperturelaboratories:~$ sudo useradd -g practica5 -s /sbin/nologin usuario1  
chell@aperturelaboratories:~$ sudo passwd usuario1  
New password:  
Retype new password:  
passwd: password updated successfully  
chell@aperturelaboratories:~$ sudo useradd -g practica5 -s /sbin/nologin usuario2  
chell@aperturelaboratories:~$ sudo passwd usuario2  
New password:  
Retype new password:  
passwd: password updated successfully  
chell@aperturelaboratories:~$
```

Grupo `practica5` usuarios `usuario1` y `usuario2`

Se verifica que los usuarios han sido creados correctamente.

```
chell@aperturelaboratories: ~  
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin  
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false  
uuuid:x:107:112::/run/uuuid:/usr/sbin/nologin  
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin  
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin  
pollinate:x:110:1::/var/cache/pollinate:/bin/false  
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin  
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin  
chell:x:1000:1000:Galán:/home/chell:/bin/bash  
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false  
bind:x:112:118::/var/cache/bind:/usr/sbin/nologin  
mysql:x:113:119:MySQL Server,,,:/nonexistent:/bin/false  
usuario1:x:1001:1001::/home/usuario1:/sbin/nologin  
usuario2:x:1002:1001::/home/usuario2:/sbin/nologin  
~  
37,1 Bot
```

Se abrió `/etc/passwd` con `vim` para verlo mejor

⚠ Estos usuarios no podrán acceder a un terminal y solo podrán acceder a sus directorios mediante un cliente SFTP.

Gestionar los permisos

Fichero principal de configuración

Se pueden añadir permisos específicos en el fichero principal de configuración de SSH, `sshd_config`, para controlar el acceso de usuarios; en este caso, para que se conecten únicamente por SFTP y a un directorio específico.

```
chell@aperturelaboratories: ~  
chell@aperturelaboratories:~$ sudo vim /etc/ssh/sshd_config  
chell@aperturelaboratories:~$
```

```
chell@aperturelaboratories: ~  
# Allow client to pass locale environment variables  
AcceptEnv LANG LC_*  
  
# override default of no subsystems  
#Subsystem sftp /usr/lib/openssh/sftp-server  
  
Subsystem sftp internal-sftp  
  
Match Group practica5  
ForceCommand internal-sftp  
PasswordAuthentication yes  
ChrootDirectory /sftp/  
  
# Example of overriding settings on a per-user basis  
#Match User anoncvs  
-- INSERT --
```

Opción por defecto señalada y comentada

La ruta `/sftp/` especificada es el comienzo de la **ruta** donde estarán las carpetas `home` de los usuarios.

Carpeta raíz y de usuarios

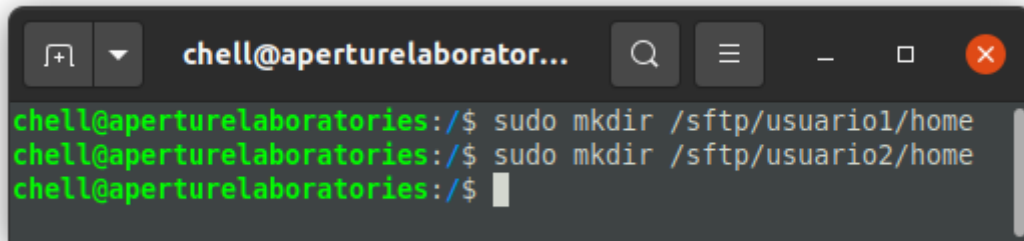
⚠ Debe crearse la carpeta raíz `/sftp/` y la de los usuarios.

También deben darse permisos de superusuario a la carpeta raíz `/sftp/` para que SSH pueda entrar, así como a los usuarios para sus carpetas.

```
chell@aperturelaboratories: /  
chell@aperturelaboratories:/$ sudo mkdir /sftp && sudo mkdir /sftp/usuario1 /sftp/usuario2  
chell@aperturelaboratories:/$ sudo chown root:root /sftp/ && sudo chmod 755 /sftp/  
chell@aperturelaboratories:/$ sudo chown usuario1:practica5 /sftp/usuario1  
chell@aperturelaboratories:/$ sudo chown usuario2:practica5 /sftp/usuario2  
chell@aperturelaboratories:/$
```

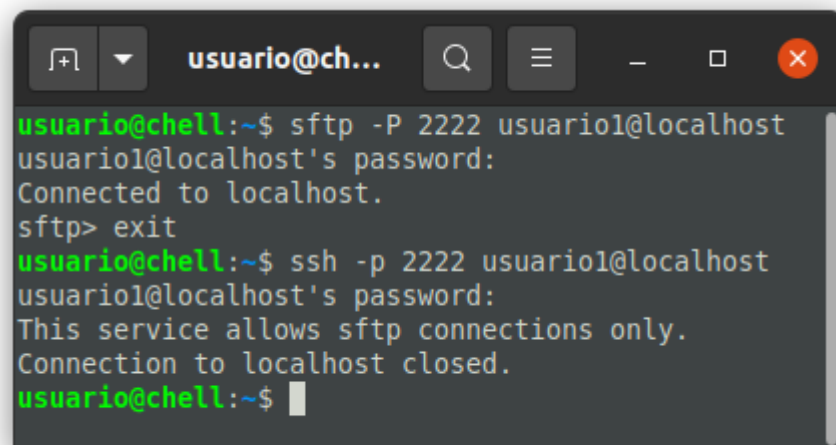
Creación de las carpetas necesarias para los apartados anteriores

Ahora, la estructura de las carpetas de los usuarios.



```
chell@aperturelaborator...  
chell@aperturelaboratories:/$ sudo mkdir /sftp/usuario1/home  
chell@aperturelaboratories:/$ sudo mkdir /sftp/usuario2/home  
chell@aperturelaboratories:/$
```

Comprobación



```
usuario@chell...  
usuario@chell:~$ sftp -P 2222 usuario1@localhost  
usuario1@localhost's password:  
Connected to localhost.  
sftp> exit  
usuario@chell:~$ ssh -p 2222 usuario1@localhost  
usuario1@localhost's password:  
This service allows sftp connections only.  
Connection to localhost closed.  
usuario@chell:~$
```

Conexión por SFTP correcta, conexión por SSH no disponible (solo SFTP)