chroot (enjaulado)

linux, ssh

los usuarios se quedan encerrados en un directorio y no pueden salir de ahí (excepciones con `mount --bind`)

sshd_config

```
# override default of no subsystems
##Subsystem     sftp    /usr/libexec/openssh/sftp-server
Subsystem       sftp    internal-sftp

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       ForceCommand cvs server

AllowGroups ConexionSFTP

Match group ConexionSFTP
ChrootDirectory /home/conexionesdftp
ForceCommand internal-sftp
```

- http://debianyderivadas.blogspot.com.es/2011/03/enjaular-sftp-algunos-usuarios.html
- http://www.esdebian.org/wiki/enjaulado-sftp

ssh chroot

- paso a paso: https://www.tecmint.com/restrict-ssh-user-to-directory-using-chrooted-jail/

```
mkdir -p /home/test
ls -l /dev/{null,zero,stdin,stdout,stderr,random,tty}
mkdir -p /home/test/dev/
cd /home/test/dev/
mknod -m 666 null c 1 3
mknod -m 666 tty c 5 0
mknod -m 666 zero c 1 5
mknod -m 666 random c 1 8
chown root:root /home/test
chmod 0755 /home/test
ls -ld /home/test
mkdir -p /home/test/bin
cp -v /bin/bash /home/test/bin/
ldd /bin/bash
mkdir -p /home/test/lib64
cp -v /lib64/{libtinfo.so.5,libdl.so.2,libc.so.6,ld-linux-x86-64.so.2}
/home/test/lib64/
useradd tecmint
passwd tecmint
mkdir /home/test/etc
```

```
cp -vf /etc/{passwd,group} /home/test/etc/
```

- vi /etc/ssh/sshd_config:

```
#define username to apply chroot jail to
Match User tecmint
#specify chroot jail
ChrootDirectory /home/test
```

- `systemctl restart sshd`

- test de conexión. Sin comandos externos.
- añadir $HOME y otros comandos:

```
mkdir -p /home/test/home/tecmint
chown -R tecmint:tecmint /home/test/home/tecmint
chmod -R 0700 /home/test/home/tecmint
cp -v /bin/ls /home/test/bin/
cp -v /bin/date /home/test/bin/
cp -v /bin/mkdir /home/test/bin/
ldd /bin/ls
cp -v
/lib64/{libselinux.so.1,libcap.so.2,libacl.so.1,libc.so.6,libpcre.so.1,libdl.s
o.2,ld-linux-x86-64.so.2,libattr.so.1,libpthread.so.0} /home/test/lib64/
```

quick reference

1. crear grupo :

```
groupadd sftpusers
```

2. añadir usuario:

```
useradd -g sftpusers -d /incoming -s /sbin/nologin guestuser; passwd guestuser
```

   - o modificar uno existente:

```
usermod -g sftpusers -d /incoming -s /sbin/nologin john
```

3. modificar **/etc/ssh/sshd_config**:

```
#Subsystem      sftp    /usr/libexec/openssh/sftp-server
Subsystem       sftp    internal-sftp
```

4. añadir al final del fichero **/etc/ssh/sshd_config**:

```
Match Group sftpusers
        ChrootDirectory /sftp/%u
        ForceCommand internal-sftp
```

   - en este caso, el directorio usado para almacenar los usuarios de SFTP es **/sftp/<user>/**
5. comprobar que esté habilitado el login por contraseña en **/etc/ssh/sshd_config**:

```
PasswordAuthentication no
```

6. crear el directorio home : en este caso

```
mkdir -p /sftp/guestuser/incoming
```

7. asignar permisos (respetar el root:root de **/sftp/** y **/sftp/guestuser/**):

```
chown guestuser:sftpusers /sftp/guestuser/incoming
```

8. reiniciar el servicio:

```
service sshd restart
```

/via: https://www.thegeekstuff.com/2012/03/chroot-sftp-setup

umask en conexiones SFTP enjauladas

método 1 (no probado):

sshd_config

```
Subsystem sftp internal-sftp -u 0002
```

http://jeff.robbins.ws/articles/setting-the-umask-for-sftp-transactions

método 2 (probado, funciona):

sshd_config

```
Subsystem sftp internal-sftp

UsePAM yes

Match user username
ChrootDirectory /path/to/directory
ForceCommand internal-sftp
```

/etc/pam.d/sshd

```
session optional pam_umask.so umask=0002
```

/etc/profile

```
umask 022 # añadir al fichero para que las sesiones interactivas tengan un
umask diferente al establecido en ''/etc/pam.d/sshd''
```

- http://sysadmin.circularvale.com/server-config/setting-a-umask-for-chrooted-sftp-users/
- otras opciones? (2019-11-11): https://rm-rf.es/configurar-umask-para-sesiones-sftp/

From:
https://matebcn.eu/ - **miguel angel torres egea**

Permanent link:
https://matebcn.eu/linux:ssh:chroot

Last update: **05/05/2026 09:44**