

chroot (enjaulado)

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

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.robins.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://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:ssh:chroot?rev=1573473152>

Last update: **11/11/2019 03:52**

