# SFTP

Sftp use ssh to transfer files securely.

If you want to setup an account on your system that will be used only to transfer files (and not to ssh to the system), you should setup SFTP Chroot Jail as explained in this article.

# Chroot SFTP Environment

## 1. Create a New Group

Create a group called sftpusers. Only users who belong to this group will be automatically restricted to the SFTP chroot environment on this system.

# groupadd sftpusers

## 2. Create Users (or Modify Existing User)

Let us say you want to create an user guestuser who should be allowed only to perform SFTP in a chroot environment, and should not be allowed to perform SSH.

The following command **creates guestuser, assigns this user to sftpusers group, make /incoming as the home directory, set /sbin/nologin as shell** (which will not allow the user to ssh and get shell access).

# useradd -g sftpusers -d /incoming -s /sbin/nologin guestuser

# passwd guestuser

Verify that the user got created properly.

# grep guestuser /etc/passwd

guestuser:x:500:500::/incoming:/sbin/nologin

If you want to modify an existing user and make him an sftp user only and put him in the chroot sftp jail, do the following:

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

## 3. Setup sftp-server Subsystem in sshd\_config

You should instruct sshd to use the internal-sftp for sftp (instead of the default sftp-server).

Modify the the /etc/ssh/sshd\_config file and comment out the following line:

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

Next, add the following line to the /etc/ssh/sshd\_config file

Subsystem sftp internal-sftp

# grep sftp /etc/ssh/sshd\_config

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

Subsystem sftp internal-sftp

## 4. Specify Chroot Directory for a Group

You want to put only certain users (i.e users who belongs to sftpusers group) in the chroot jail environment. Add the following lines at the end of /etc/ssh/sshd\_config

# tail /etc/ssh/sshd\_config

Match Group sftpusers

ChrootDirectory /sftp/%u

ForceCommand internal-sftp

In the above:

* Match Group sftpusers – This indicates that the following lines will be matched only for users who belong to group sftpusers
* ChrootDirectory /sftp/%u – This is the path that will be used for chroot after the user is authenticated. %u indicates the user. So, for john, this will be /sftp/john.
* ForceCommand internal-sftp – This forces the execution of the internal-sftp and ignores any command that are mentioned in the ~/.ssh/rc file.

## 5. Create sftp Home Directory

Since we’ve specified /sftp as ChrootDirectory above, create this directory (which iw equivalent of your typical /home directory).

# mkdir /sftp

Now, under /sftp, create the individual directories for the users who are part of the sftpusers group. i.e the users who will be allowed only to perform sftp and will be in chroot environment.

# mkdir /sftp/guestuser

So, /sftp/guestuser is equivalent to / for the guestuser. When guestuser sftp to the system, and performs “cd /”, they’ll be seeing only the content of the directories under “/sftp/guestuser” (and not the real / of the system). This is the power of the chroot.

So, under this directory /sftp/guestuser, create any subdirectory that you like user to see. For example, create a incoming directory where users can sftp their files.

# mkdir /sftp/guestuser/incoming

## 6. Setup Appropriate Permission

For chroot to work properly, you need to make sure appropriate permissions are setup properly on the directory you just created above.

Set the owenership to the user, and group to the sftpusers group as shown below.

# chown guestuser:sftpusers /sftp/guestuser/incoming

The permission will look like the following for the incoming directory.

# ls -ld /sftp/guestuser/incoming

drwxr-xr-x 2 guestuser sftpusers 4096 Dec 28 23:49 /sftp/guestuser/incoming

The permission will look like the following for the /sftp/guestuser directory

# ls -ld /sftp/guestuser

drwxr-xr-x 3 root root 4096 Dec 28 23:49 /sftp/guestuser

# ls -ld /sftp

drwxr-xr-x 3 root root 4096 Dec 28 23:49 /sftp