User can only scp files with no shell access

Ein lokaler User, soll sich legendlich auf dem Server in einem für ihn eingerichteten Ordner via SCP einloggen und dort seine files kopieren, löschen und verwalten können. **(Er darf sich nicht auf eine Shell verbinden!)**

Konfiguration

1. Create a new user (sftptest) and make their shell /sbin/nologin:

```
# useradd -s /sbin/nologin sftptest
```

2. Add a new group (sftponly) and add the user to that group:

```
# groupadd sftponly
# usermod -g sftponly sftptest
```

3. Change permissions of the users home dir to be as follows:

```
# chown root:root /home/sftptest
# chmod 755 /home/sftptest
```

4. Make a directory for the user (sftptest) to be able to scp to (a destination directory):

```
# mkdir /home/sftptest/incoming
# chown sftptest:sftptest /home/sftptest/incoming
```

5. Set the password for the sftptest user.

```
 # passwd sftptest
```

6. Add the following to /etc/ssh/sshd_config:

```
 # vim /etc/ssh/sshd_config
```

```
Match group sftponly
       ChrootDirectory %h
       X11Forwarding no
       AllowTcpForwarding no
       ForceCommand internal-sftp
```

NOTE: The sshd stanza can be adjusted in three basic modes:

- Using the **%h** directive to lock each user into their own home directory (see above example)
- Or using a single hardcoded directory name → `ChrootDirectory /home/user/`
- Keep in mind: There is no need, to create an Group, if just one user should be able to have Access. In this case replace “Match group sftponly” with “Match user sftptest”

After all changes, restart sshd!

```
# systemctl restart sshd
```

Last update: **2017/11/06 14:30**