**INSTALL AND CONFIGURE Sftp Service**

1. Create the directories for the user for example:

#cd /data2/

#mkdir SFTP (to host all Sftp users home dirs)

#mkdir SFTP/ftp\_<user> (create specific user home directory)

#mkdir SFTP/ftp\_<user>/uplod (create upload directory in home)

1. Create group for Sftp users:

#groupadd sftp\_users

1. Create user:

#useradd <user> -d /data2/SFTP/ftp\_<user>

Passwd <user>

1. Attach user to sftp\_users group:

Add the user name to /etc/group file to end of the sftp\_users line separated with comas if more then one

1. Set permissions on the directories:

/data2 -> 755 root:root

/data2/SFTP -> 755 root:root

/data2/SFTP/ftp<user> -> 755 root:sftp\_users

/data2/SFTP/ftp<user>/upload -> 755 <user>:<sftp\_users>

1. Edit /etc/ssh/sshd config as following for jailing users to their home directory:

Comment the line “Subsystem sftp /usr/libexec/openssh/sftp-server”

Add the line “Subsystem sftp internal-sftp”

Add the following block to end of file:

“Match Group sftp\_users

PasswordAuthentication yes

ChrootDirectory %h

AllowTCPForwarding no

X11Forwarding no

ForceCommand internal-sftp”

1. For security add second interface to server so regular ssh will be on port 22 and Sftp will be on example port 990.
2. Configure /etc/ssh/sshd\_config as following:

Comment the line : “Port 22”

Add the following lines:

ListenAddress internal-ip-1:22

ListenAddress internal-ip-2-2:990

1. Restart sshd service