# 

[**UBUNTU 16.04**](#_tavses7paza2) **1**

[Password based SFTP:](#_mgg5f9lbbwec) 1

[Step 1: Check openSSH setup](#_ewbuw2tyz4qb) 1

[Step 2: Checking OpenBSD Secure Shell server](#_e027ogmdcznd) 3

[Step 3: Addition of SFTP user group](#_u2g0ncisuuiz) 4

[Step 4: Create the main sftp folder](#_3y22ad602hpq) 5

[Step 5: Create user's home folder](#_jszgtw2nen22) 5

[Step 6: Create User, set home folder and assign it to the sftp group](#_941s5tpffznr) 5

[6.1 Create a user, add to group](#_fmau593818fz) 5

[6.2: Change user password](#_y4pcu42q9cm3) 6

[6.3 Give ownership of the folder to the user created](#_uyr3w3lw7489) 6

[Step 7: Add subsystem sftp and Secure the sftp](#_dicfubnwr9m4) 6

[7.1 Add the following lines towards the end of file /etc/ssh/sshd\_config.](#_rh5lsqcwq8ln) 6

[7.2 Find any already existing subsystem and comment it](#_h4y0yw8lv85w) 6

[7.3 And add the following in the end:](#_b5jli5kpbwqb) 7

[Step 8: Restart the ssh server](#_zf11n5j98u53) 7

[Debugging:](#_shejpc5a0m2) 7

# 

# UBUNTU 16.04

## Password based SFTP:

### Step 1: Check openSSH setup

In general, OpenSSH comes built-in with most of the Linux systems. Check whether port 22 is opened or not

ssh -v localhost

**Scenario 1:**

If you get the following output:

|  |
| --- |
| sensen@hyd-dev-lp-13:~$ ssh -v localhost  OpenSSH\_7.2p2 Ubuntu-4ubuntu2.8, OpenSSL 1.0.2g 1 Mar 2016  debug1: Reading configuration data /etc/ssh/ssh\_config  debug1: /etc/ssh/ssh\_config line 19: Applying options for \*  debug1: Connecting to localhost [127.0.0.1] port 22.  debug1: connect to address 127.0.0.1 port 22: Connection refused  ssh: connect to host localhost port 22: Connection refused |

It would mean the connection is not successful. You can debug the cause but for me I removed and reinstalled the open ssh using the following commands:

--Removal

sudo apt-get remove openssh-client openssh-server

--Install

sudo apt-get install openssh-client openssh-server

**Scenario 2:**

If you directly get the following reply then no need to uninstall and reinstall as mentioned in step 1. Directly move to step 2

|  |
| --- |
| sensen@hyd-dev-lp-13:~$ ssh -v localhost  OpenSSH\_7.2p2 Ubuntu-4ubuntu2.8, OpenSSL 1.0.2g 1 Mar 2016  debug1: Reading configuration data /etc/ssh/ssh\_config  debug1: /etc/ssh/ssh\_config line 19: Applying options for \*  debug1: Connecting to localhost [127.0.0.1] port 22.  debug1: Connection established.  debug1: identity file /home/sensen/.ssh/id\_rsa type 1  debug1: key\_load\_public: No such file or directory  debug1: identity file /home/sensen/.ssh/id\_rsa-cert type -1  debug1: key\_load\_public: No such file or directory  debug1: identity file /home/sensen/.ssh/id\_dsa type -1  debug1: key\_load\_public: No such file or directory  debug1: identity file /home/sensen/.ssh/id\_dsa-cert type -1  debug1: key\_load\_public: No such file or directory  debug1: identity file /home/sensen/.ssh/id\_ecdsa type -1  debug1: key\_load\_public: No such file or directory  debug1: identity file /home/sensen/.ssh/id\_ecdsa-cert type -1  debug1: key\_load\_public: No such file or directory  debug1: identity file /home/sensen/.ssh/id\_ed25519 type -1  debug1: key\_load\_public: No such file or directory  debug1: identity file /home/sensen/.ssh/id\_ed25519-cert type -1  debug1: Enabling compatibility mode for protocol 2.0  debug1: Local version string SSH-2.0-OpenSSH\_7.2p2 Ubuntu-4ubuntu2.8  debug1: Remote protocol version 2.0, remote software version OpenSSH\_7.2p2 Ubuntu-4ubuntu2.8  debug1: match: OpenSSH\_7.2p2 Ubuntu-4ubuntu2.8 pat OpenSSH\* compat 0x04000000  debug1: Authenticating to localhost:22 as 'sensen'  debug1: SSH2\_MSG\_KEXINIT sent  debug1: SSH2\_MSG\_KEXINIT received  debug1: kex: algorithm: curve25519-sha256@libssh.org  debug1: kex: host key algorithm: ecdsa-sha2-nistp256  debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none  debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none  debug1: expecting SSH2\_MSG\_KEX\_ECDH\_REPLY  debug1: Server host key: ecdsa-sha2-nistp256 SHA256:Oc38yQQ1K33hUSeJslA6F53nOOXubRHToziissROhbo  The authenticity of host 'localhost (127.0.0.1)' can't be established.  ECDSA key fingerprint is SHA256:Oc38yQQ1K33hUSeJslA6F53nOOXubRHToziissROhbo.  Are you sure you want to continue connecting (yes/no)? y  Please type 'yes' or 'no': yes  Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.  debug1: rekey after 134217728 blocks  debug1: SSH2\_MSG\_NEWKEYS sent  debug1: expecting SSH2\_MSG\_NEWKEYS  debug1: SSH2\_MSG\_NEWKEYS received  debug1: rekey after 134217728 blocks  debug1: SSH2\_MSG\_EXT\_INFO received  debug1: kex\_input\_ext\_info: server-sig-algs=<rsa-sha2-256,rsa-sha2-512>  debug1: SSH2\_MSG\_SERVICE\_ACCEPT received  debug1: Authentications that can continue: publickey,password  debug1: Next authentication method: publickey  debug1: Offering RSA public key: /home/sensen/.ssh/id\_rsa  debug1: Authentications that can continue: publickey,password  debug1: Trying private key: /home/sensen/.ssh/id\_dsa  debug1: Trying private key: /home/sensen/.ssh/id\_ecdsa  debug1: Trying private key: /home/sensen/.ssh/id\_ed25519  debug1: Next authentication method: password  sensen@localhost's password:  debug1: Authentication succeeded (password).  Authenticated to localhost ([127.0.0.1]:22).  debug1: channel 0: new [client-session]  debug1: Requesting no-more-sessions@openssh.com  debug1: Entering interactive session.  debug1: pledge: network  debug1: client\_input\_global\_request: rtype hostkeys-00@openssh.com want\_reply 0  debug1: Sending environment.  debug1: Sending env LANG = en\_IN  Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-60-generic x86\_64)  \* Documentation: https://help.ubuntu.com  \* Management: https://landscape.canonical.com  \* Support: https://ubuntu.com/advantage  83 packages can be updated.  0 updates are security updates.  The programs included with the Ubuntu system are free software;  the exact distribution terms for each program are described in the  individual files in /usr/share/doc/\*/copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  applicable law. |

### Step 2: Checking OpenBSD Secure Shell server

This too somes built-in with ubuntu packages but to verify we can just confirm whether the service is running properly or not.

sudo service ssh status

|  |
| --- |
| sensen@hyd-dev-lp-13:~$ sudo service ssh status  [sudo] password for sensen:  ● ssh.service - OpenBSD Secure Shell server  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)  Active: active (running) since Wed 2019-09-18 09:47:48 IST; 45min ago  Process: 32235 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)  Process: 32229 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)  Main PID: 29782 (sshd)  CGroup: /system.slice/ssh.service  └─29782 /usr/sbin/sshd -D  Sep 18 10:12:12 hyd-dev-lp-13 sshd[29782]: Server listening on :: port 22.  Sep 18 10:12:12 hyd-dev-lp-13 systemd[1]: Reloading OpenBSD Secure Shell server.  Sep 18 10:12:12 hyd-dev-lp-13 sshd[29782]: Received SIGHUP; restarting.  Sep 18 10:12:12 hyd-dev-lp-13 systemd[1]: Reloaded OpenBSD Secure Shell server.  Sep 18 10:12:12 hyd-dev-lp-13 sshd[29782]: Server listening on 0.0.0.0 port 22.  Sep 18 10:12:12 hyd-dev-lp-13 sshd[29782]: Server listening on :: port 22.  Sep 18 10:24:47 hyd-dev-lp-13 sshd[32700]: Accepted password for sensen from 127.0.0.1 port 54154 ssh2  Sep 18 10:24:47 hyd-dev-lp-13 sshd[32700]: pam\_unix(sshd:session): session opened for user sensen by (uid=0)  Sep 18 10:26:40 hyd-dev-lp-13 sshd[413]: Accepted password for sensen from 127.0.0.1 port 54196 ssh2  Sep 18 10:26:40 hyd-dev-lp-13 sshd[413]: pam\_unix(sshd:session): session opened for user sensen by (uid=0) |

### 

If there are problems during this step, you need to debug it. Most probably, if you have recently done a fresh install of openSSH, you will see the service running.

If you encounter problems like the one given below:

|  |
| --- |
| sensen@hyd-dev-lp-13:/sftp$ sudo service ssh status  ● ssh.service - OpenBSD Secure Shell server  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)  Active: failed (Result: start-limit-hit) since Wed 2019-09-18 11:55:34 IST; 44s ago  Process: 32235 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)  Process: 32229 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)  Process: 5058 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=255)  Main PID: 29782 (code=exited, status=0/SUCCESS)  Sep 18 11:55:33 hyd-dev-lp-13 systemd[1]: Failed to start OpenBSD Secure Shell server.  Sep 18 11:55:33 hyd-dev-lp-13 systemd[1]: ssh.service: Unit entered failed state.  Sep 18 11:55:33 hyd-dev-lp-13 systemd[1]: ssh.service: Failed with result 'exit-code'.  Sep 18 11:55:34 hyd-dev-lp-13 systemd[1]: ssh.service: Service hold-off time over, scheduling restart.  Sep 18 11:55:34 hyd-dev-lp-13 systemd[1]: Stopped OpenBSD Secure Shell server.  Sep 18 11:55:34 hyd-dev-lp-13 systemd[1]: ssh.service: Start request repeated too quickly.  Sep 18 11:55:34 hyd-dev-lp-13 systemd[1]: Failed to start OpenBSD Secure Shell server.  Sep 18 11:55:34 hyd-dev-lp-13 systemd[1]: ssh.service: Unit entered failed state.  Sep 18 11:55:34 hyd-dev-lp-13 systemd[1]: ssh.service: Failed with result 'start-limit-hit'. |

Then check the /etc/ssh/sshd\_config file for any problems

### Step 3: Addition of SFTP user group

Assign the users that will use the sftp

|  |
| --- |
| ## Check whether a group is already present or not:  sensen@hyd-dev-lp-13:~$ grep sftp /etc/group  ## If nothing is displayed, then use the command below to add a group  sensen@hyd-dev-lp-13:~$ sudo addgroup sftp  [sudo] password for sensen:  Adding group `sftp' (GID 1000) ...  Done.  ##Verify that the new group that you added is added successfully  sensen@hyd-dev-lp-13:~$ grep sftp /etc/group  sftp:x:1000: |

### Step 4: Create the main sftp folder

|  |
| --- |
| *##This will create a directory in the root mount*  *sensen@hyd-dev-lp-13:~$ sudo mkdir /sftp*  *[sudo] password for sensen:*  *##Verify whether the directory is created or not*  *sensen@hyd-dev-lp-13:~$ ls -l*  *drwxr-xr-x 2 root root 4096 Sep 18 11:07 sftp* |

### Step 5: Create user's home folder

|  |
| --- |
| *sensen@hyd-dev-lp-13:~$ sudo mkdir /sftp/pranav*  *##Verify*  *sensen@hyd-dev-lp-13:~$ ls -l /sftp*  *total 4*  *drwxr-xr-x 2 root root 4096 Sep 18 11:14 pranav*  *##Create a working directory*  *sensen@hyd-dev-lp-13:~$ sudo mkdir /sftp/pranav/workingDir*  *##Verify*  *sensen@hyd-dev-lp-13:/sftp/pranav$ ll*  *total 12*  *drwxr-xr-x 3 root root 4096 Sep 18 15:11 ./*  *drwxr-xr-x 3 root root 4096 Sep 18 15:10 ../*  *drwxr-xr-x 2 root root 4096 Sep 18 15:11 workingDir/* |

You can create further folders as required. It is essential that the structure follows the norms specified by www.

### Step 6: Create User, set home folder and assign it to the sftp group

#### 6.1 Create a user, add to group

|  |
| --- |
| *sensen@hyd-dev-lp-13:~$ sudo useradd -d /sftp/pranav -G sftp pranav --shell /usr/sbin/nologin*  *sensen@hyd-dev-lp-13:~$ grep sftp /etc/group*  *Sftp:x:1000:pranav*  *sensen@hyd-dev-lp-13:~$ sudo su pranav*  *This account is currently not available.* |

#### 6.2: Change user password

Please note that echo -e will be piped into the next command to set the password so a \n is required to fill the password first and then its confirmation.

|  |
| --- |
| *sensen@hyd-dev-lp-13:~$ echo -e "test\ntest" | sudo passwd pranav*  *Enter new UNIX password: Retype new UNIX password: passwd: password updated successfully* |

If you do not enter the password correctly or entered it without giving a \n you may get errors. Please ensure you use the above commands only.

#### 6.3 Give ownership of the folder to the user created

|  |
| --- |
| *sensen@hyd-dev-lp-13:/sftp$ sudo chown pranav:sftp -R /sftp/pranav/workingDir*  *##Verify the ownership*  *sensen@hyd-dev-lp-13:~$ ls -l /sftp/pranav/*  *total 4*  *drwxr-xr-x 2 pranav sftp 4096 Sep 18 15:11 workingDir* |

### Step 7: Add subsystem sftp and Secure the sftp

#### 7.1 Add the following lines towards the end of file /etc/ssh/sshd\_config.

sudo nano /etc/ssh/sshd\_config

#### 7.2 Find any already existing subsystem and comment it

Subsystem sftp /usr/lib/openssh/sftp-server # This path can be any standard path

After commenting it should look like the following:

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

The motivation behind doing this is that sometimes these original subsystems use bash\_rc adn other important files which we do not need

#### 7.3 And add the following in the end:

Subsystem sftp internal-sftp

Match Group sftp #Change this name if you your any other name for the group other than sftp

ChrootDirectory %h # Prevent user access to anything beyond their home folder

X11Forwarding no # Disable X11 forwarding

AllowTcpForwarding no # Disable tunneling

AllowAgentForwarding no # Disable port forwarding

PermitTunnel no # Disable network tunneling

ForceCommand internal-sftp # Force the connection to use the built-in SFTP server

If you do not find the line in 7.2 then add it along with the group information towards the end of the file.

### 

### Step 8: Restart the ssh server

sudo service ssh restart

If you have done any mistake in changing the sshd\_config file then it might happen that the service may not be up.

|  |
| --- |
| *//If it fails you may get responses like this.*  *sensen@hyd-dev-lp-13:/sftp$ sudo service ssh restart*  *Job for ssh.service failed because the control process exited with error code. See "systemctl status ssh.service" and "journalctl -xe" for details.* |

Correct the mistakes and it will be up again

## Debugging:

If there are authentication errors like

|  |
| --- |
| sensen@hyd-dev-lp-13:~$ sftp pranav@localhost  pranav@localhost's password:  packet\_write\_wait: Connection to 127.0.0.1 port 22: Broken pipe  Couldn't read packet: Connection reset by peer |

Use the following command to get to know the root cause of the issue

**cat /var/log/auth.log**

If you see the following line:

|  |
| --- |
| Sep 18 15:01:57 hyd-dev-lp-13 sshd[3933]: fatal: bad ownership or modes for chroot directory "/sftp/dirName" |

Then you need to delete the user (from System settings) and the related files and start fresh from step 5.

The reason behind this is that the folder hierarchy that you defined and the owners that you put have is not correct in accordance to :

***All components of the pathname must be root-owned directories that are not writable by any other user or group***

The above is in according to open bsd standards

[OpenBSD Man Page link](http://man.openbsd.org/sshd_config)