Create SFTP user and Jail it to the home dir

- If in our system sshd in not available then install using below command:
  sudo install openssh-server.

```
nishit@nishit-VirtualBox:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-server is already the newest version (1:8.2p1-4ubuntu0.5).
The following packages were automatically installed and are no longer required:
  libc-ares2 libpcre2-posix2 libzip5 php7.4-dev php7.4-gd php7.4-mysql php7.4-xml php7.4-xmlrpc php7.4-zip
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 56 not upgraded.
```

- Start sshd and check the status:
  sudo systemctl start sshd
  sudo systemctl status sshd

```
nishit@nishit-VirtualBox:~$ sudo systemctl start sshd
nishit@nishit-VirtualBox:~$ sudo systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-02-23 10:35:47 IST; 3s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 15173 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 15174 (sshd)
      Tasks: 1 (limit: 7429)
     Memory: 1.0M
     CGroup: /system.slice/ssh.service
             └─15174 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Feb 23 10:35:47 nishit-VirtualBox systemd[1]: Starting OpenBSD Secure Shell server...
Feb 23 10:35:47 nishit-VirtualBox sshd[15174]: Server listening on 0.0.0.0 port 22.
Feb 23 10:35:47 nishit-VirtualBox sshd[15174]: Server listening on :: port 22.
Feb 23 10:35:47 nishit-VirtualBox systemd[1]: Started OpenBSD Secure Shell server.
```

- Create one group in that add one user using below command:
  sudo groupadd groupdemo
  sudo useradd -g groupdemo -s /bin/false -m -d /home/userdemo1 userdemo1
  sudo usermod -G groupdemo -s /bin/false userdemo1

```
nishit@nishit-VirtualBox:~$ sudo groupadd groupdemo
[sudo] password for nishit:
```

```
nishit@nishit-VirtualBox:~$ sudo useradd -g groupdemo -s /bin/false -m -d /home/userdemo1 userdemo1
nishit@nishit-VirtualBox:~$ sudo usermod -G groupdemo -s /bin/false userdemo1
```

-s *bin*/false means user can't login to server through SSH.
-m -d /home/username means useradd to create the user home directory.

- Here we need to set user home directory compolsory provide root ownership and 755 permission:

  sudo chown root: /home/userdemo1

  sudo chmod 755 /home/userdemo1

```
nishit@nishit-VirtualBox:~$ sudo chown root: /home/userdemo1
nishit@nishit-VirtualBox:~$ sudo chmod 755 /home/userdemo1
```

- Create some directory under /*home*/username and give 755 permission and user must connect with group.
  sudo mkdir /home/userdemo1/mydir
  sudo chmod 755 /home/userdemo1/mydir
  sudo chown userdemo1:groupdemo /home/userdemo1/mydir

```
nishit@nishit-VirtualBox:~$ sudo mkdir /home/userdemo1/mydir
nishit@nishit-VirtualBox:~$ sudo chmod 755 /home/userdemo1/mydir
nishit@nishit-VirtualBox:~$ sudo chown userdemo1:groupdemo /home/userdemo1/mydir
```

- Now set user strong password.
  sudo passwd userdemo1

```
nishit@nishit-VirtualBox:~$ sudo passwd userdemo1
New password:
Retype new password:
passwd: password updated successfully
```

- Open ssh configuration file and with adding below containt:
  sudo nano /etc/ssh/sshd_config

```
nishit@nishit-VirtualBox:~$ sudo nano /etc/ssh/sshd_config
```

Configuration file containt:

subsystem sftp internal-sftp
Match Group groupdemo
ChrootDirectory /home
ForceCommand internal-sftp
#AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no

subsystem sftp internal-sftp: Mening of this line is configuration for the OpenSSH server's SFTP subsystem. It defines a subsystem named "internal-sftp" and sets various options mention in below.

Match Group groupdemo: This line meaning is the group named "groupdemo" will only apply to users who are members of that group (means userdemo1).

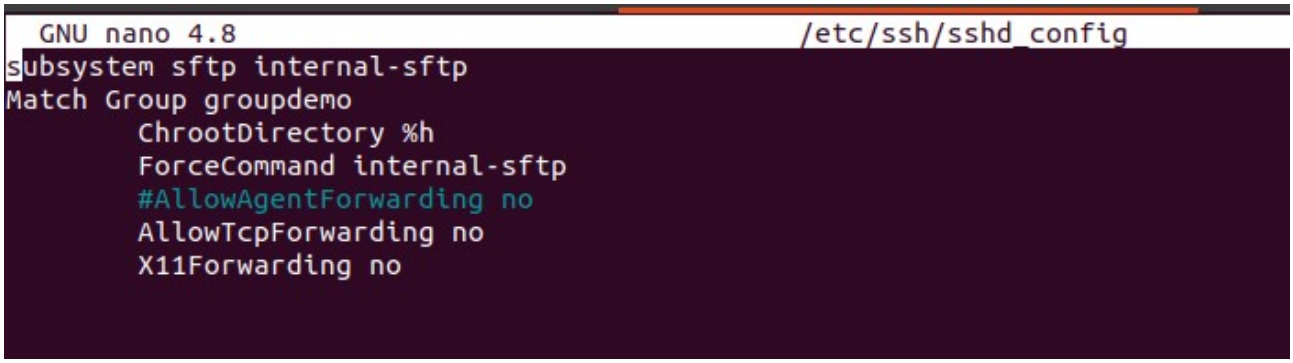
ChrootDirectory /home: This line sets the root directory for the SFTP session to /home. This means that users in the "groupdemo" will not be able to access outside of directory.

ForceCommand internal-sftp: Meaning of this line is user should not be able to execute arbitrary commands.

AllowTcpForwarding no: This means that user will not be able to create TCP connections to other systems.

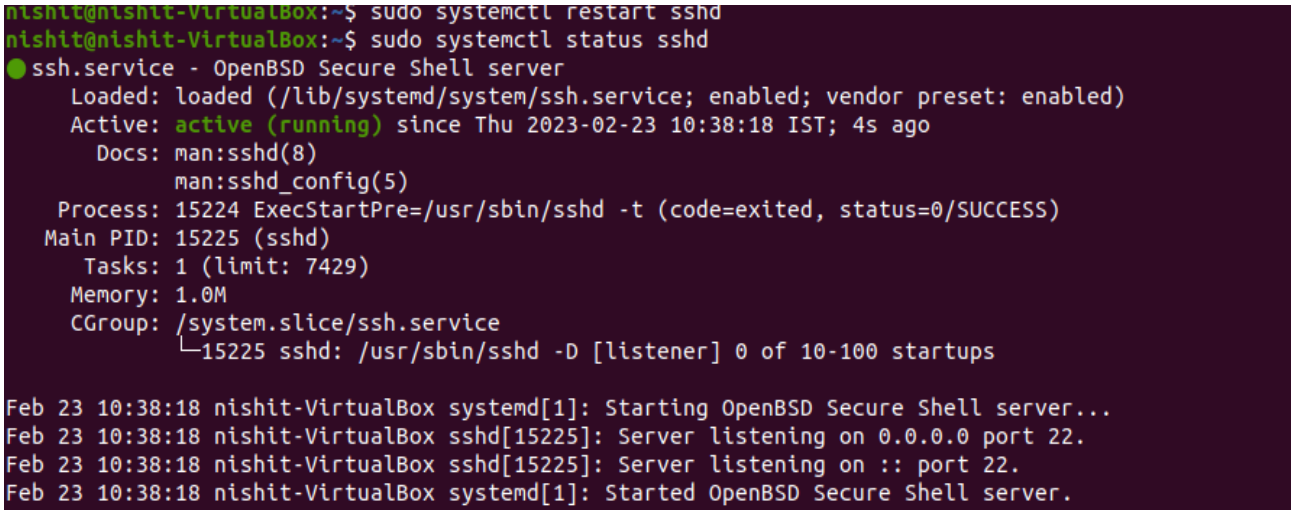
X11Forwarding no: This means that user will not be able to run graphical applications remotely.

Save and exit to file using ctrl+s & ctrl+x.



- Now restart sshd service and check the status:

sudo systemctl start sshd
sudo systemctl status sshd



- Now, access sftp using another system using below command:
  sftp userdemo1@192.168.10.133

That means we are trying to access sftp using user userdemo1 and ip address will 192.168.10.133.

- **Here, we see while entering “ls” command we get same directory that we are created that means we only have access of user’s home directory.**