Server

Task 1: Setup

1. Server Administrator Tasks (VM1):

- Create local user accounts for each client on the server.

**Client1:**

sudo useradd -m client1

sudo passwd client1

New password: client1

**Client2:**

sudo useradd -m client2

sudo passwd client2

New password: client2

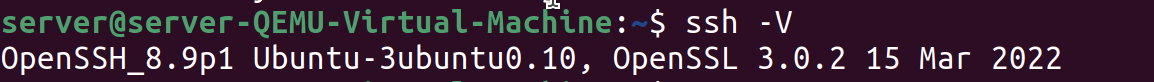
- Install and enable SSHD.

sudo apt install openssh-server

sudo systemctl enable ssh

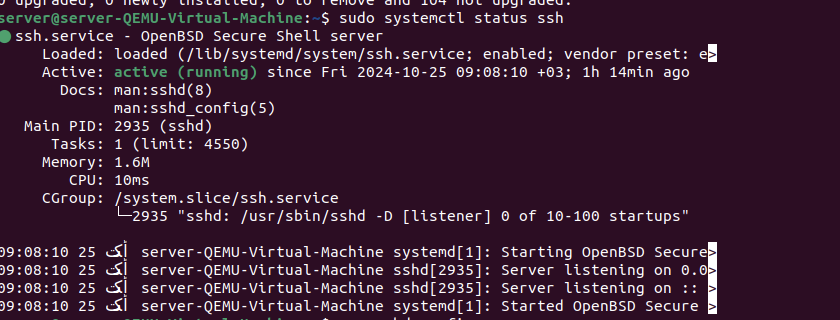
**- To check SSHD**

ssh -V



**Verify:**

sudo systemctl status ssh



- Configure SFTP for file transfer operations.

sudo nano /etc/ssh/sshd\_config

**ip address of current server:**

ifconfig

192.168.64.3

ssh [server@192.168.64.3](mailto:server@192.168.64.3)

**-Secure SFTP to client1 and client2 only**

sudo nano /etc/ssh/sshd\_config

*[at the end we modify and write the folowwing to ensure SFTP is restricted to client1 and client2 only]*

Match User clien1,client2

ForceCommand internal-sftp

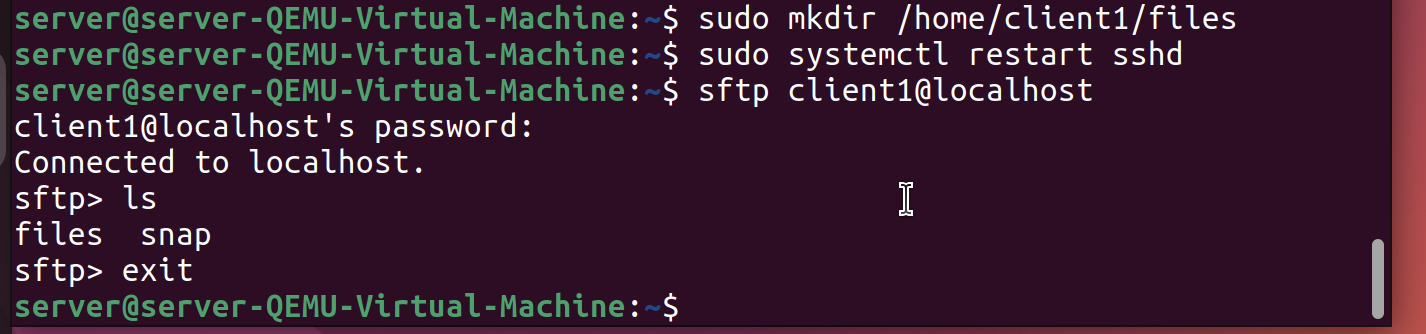
ChrootDirectory /home/%u

AllowTCPForwarding no

X11Forwarding no

**-Try to connect client1 and client2 via SFTP**

sftp client1@localhost



**if they fail to get connected, we ensure that clients have 755 permision and should be owned by root. This will also ensure they can download and upload files**

A screenshot of a computer program

Description automatically generated

Task 2: Configuration

1. Server Configuration (VM1):

**• SSH and SFTP Configuration:**

* Enable SSH access for clients using local account credentials, that is, configure SSHD server such that clients can access any file via their local accounts, using username and password.

sudo nano /etc/ssh/sshd\_config

PasswordAuthentication and set it to yes

A blue text on a black background

Description automatically generated

Since, at the beginning, clients were made to access only sftp connection, while trying to connect localhost via ssh we will be denied.

A computer screen shot of white text

Description automatically generated

to fix this error we modify the permissions in the sshd\_config by removing ForceCommand internal-sftp from the following:

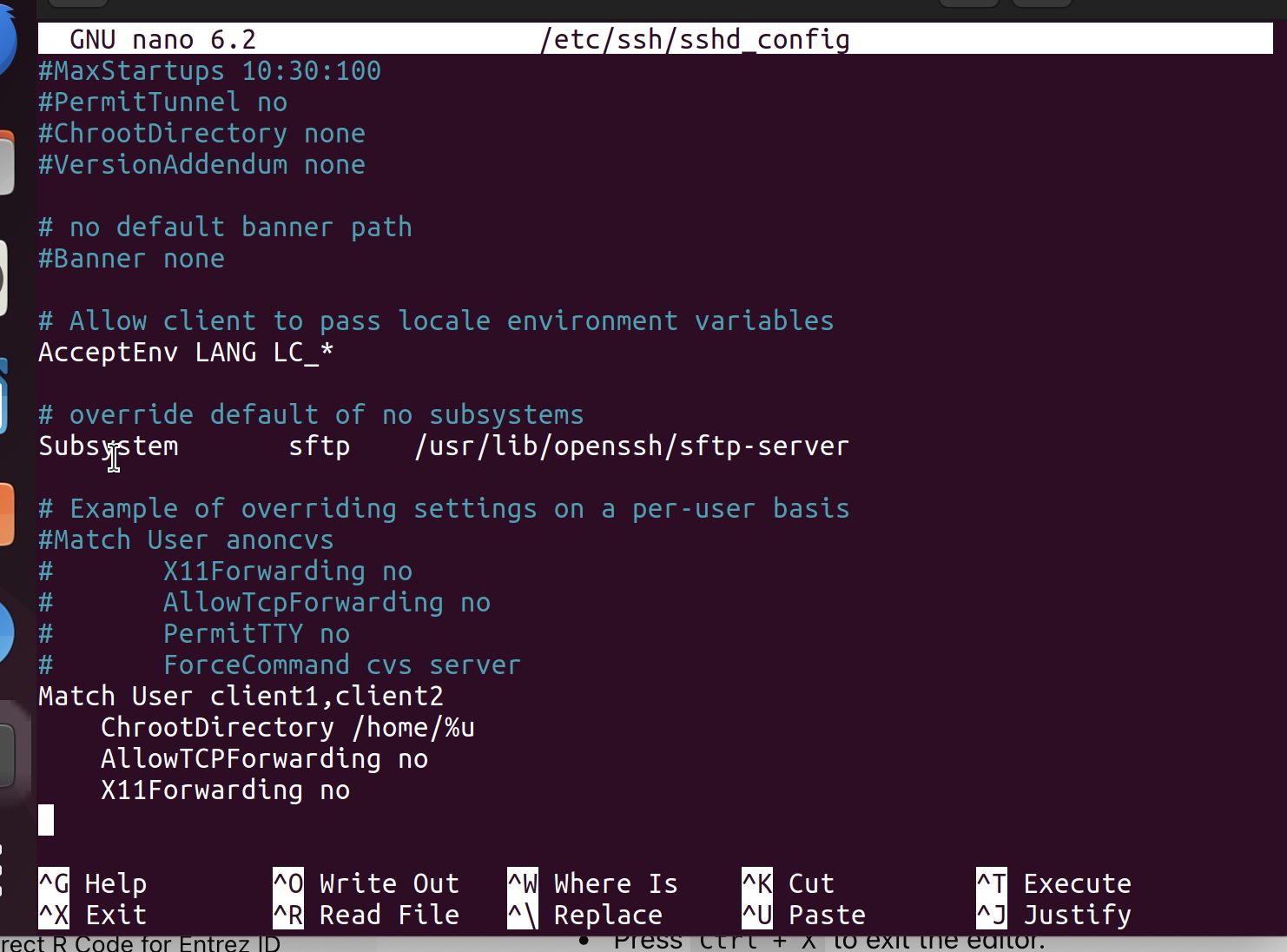
Match User clien1,client2

ForceCommand internal-sftp

ChrootDirectory /home/%u

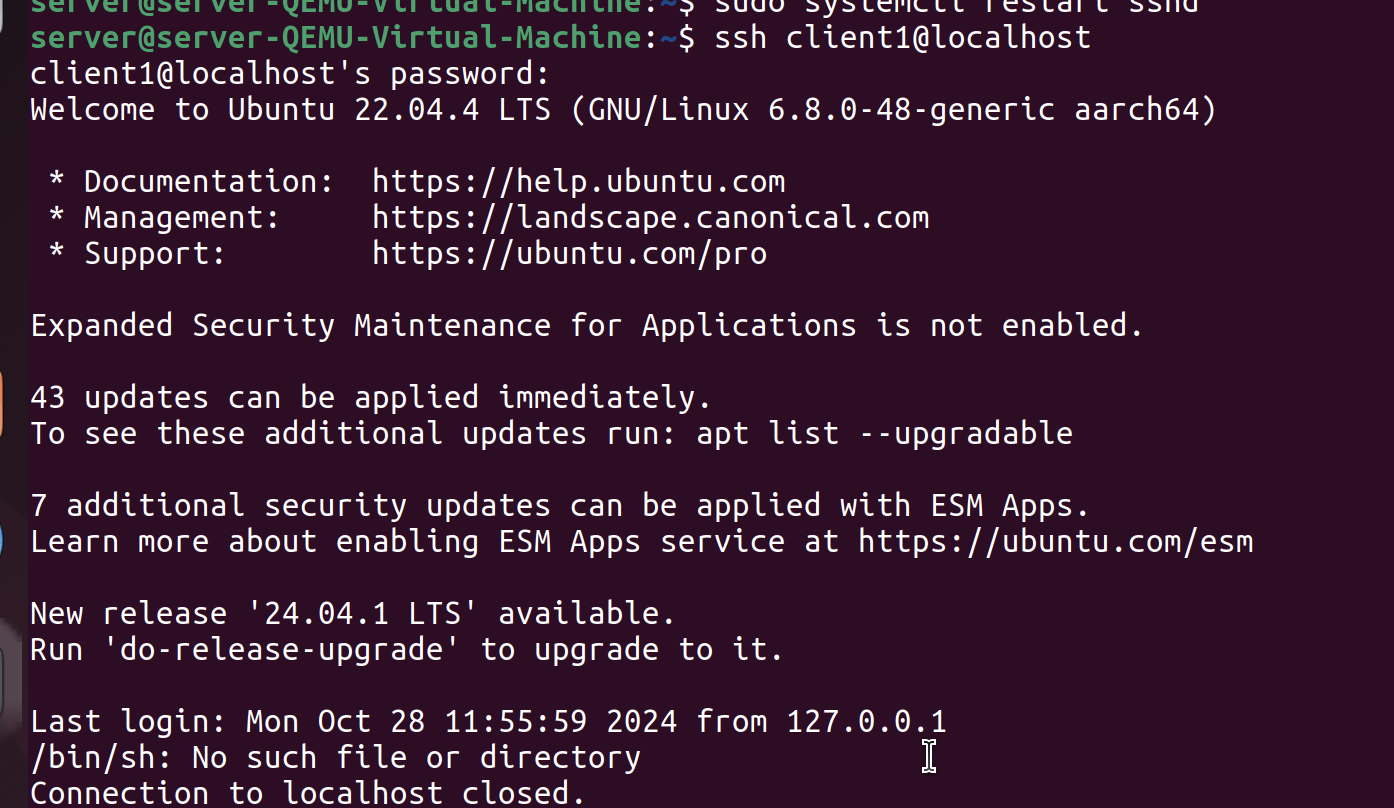
AllowTCPForwarding no

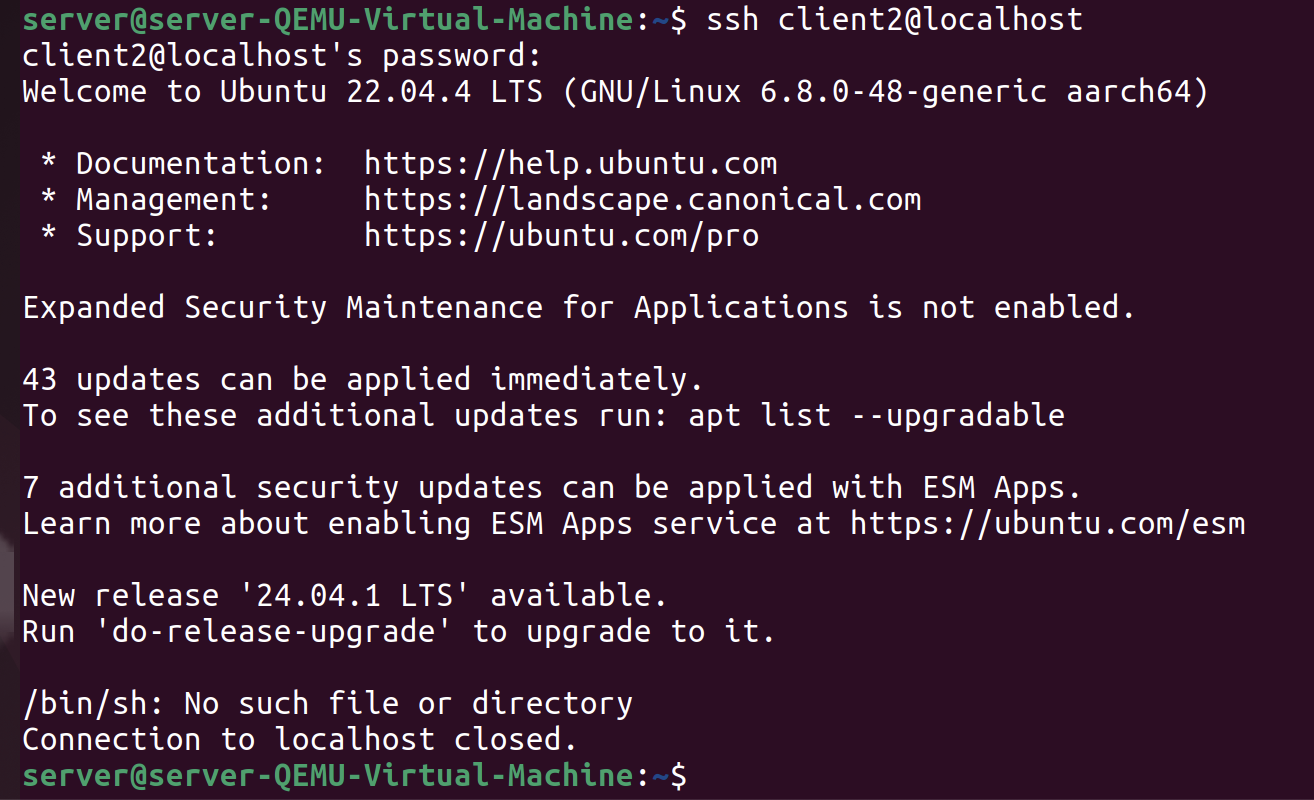
X11Forwarding no



*Removing the whole match user command will ensure clients have acces to both SSH and SFTP*

*Testing:*





* Set up SFTP for file uploads/downloads.

**client1:**

sudo chown root:root /home/client1

sudo chmod 755 /home/client1

sudo mkdir /home/client1/filesClient1.txt

**client2:**

sudo chown root:root /home/client2

sudo chmod 755 /home/client2

sudo mkdir /home/client2/filesClient2.txt

* Secure copy will be used to transfer files to and from server.

*Secure copy protocol (SCP) is a command that allows for efficient and secure file transfers between two systems across a network. It employs Secure Shell (SSH) to authenticate systems and encrypt data.sf*

**Syntax:** scp [options] [source username@IP]:/[directory and file name] [destination username@IP]:/[destination directory]

*since I am testing all these things in same local machine, ip address of my clients and server is same*

**to copy file: “fileServer.txt” from server to client1:**

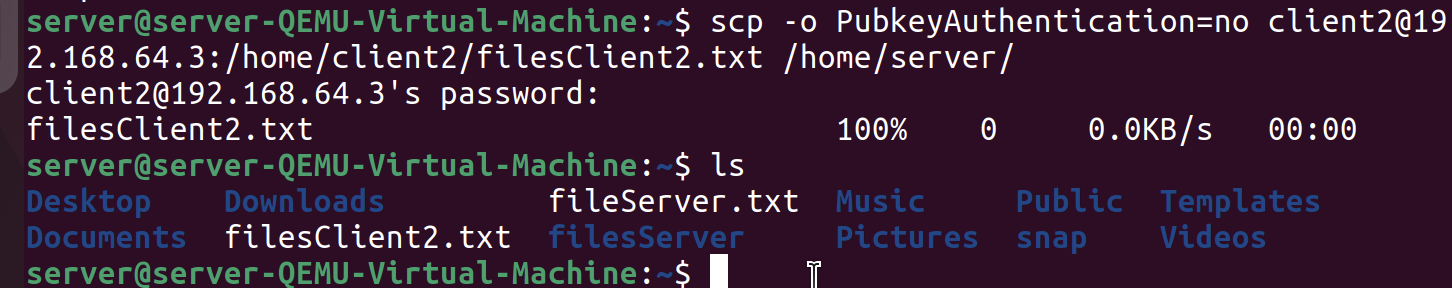
scp fileServer.txt client1@192.168.64.3:/home/client1/

A screen shot of a computer

Description automatically generated

**to copy file: “fileClient2.txt” from client2exit to server:**

scp -o PubkeyAuthentication=no [client2@192.168.64.3:/home/client2/filesClient2.txt /home/server/](mailto:client2@192.168.64.3:/home/client2/filesClient2.txt%20/home/server/)



we used -o so that while pasting in server, it doesn’t show error about denied permission due to public key and password

Task 3: Shell Scripting

**Server Side Shell script 1: (Network.sh)**

Server Side Shell script 2: (System.sh)