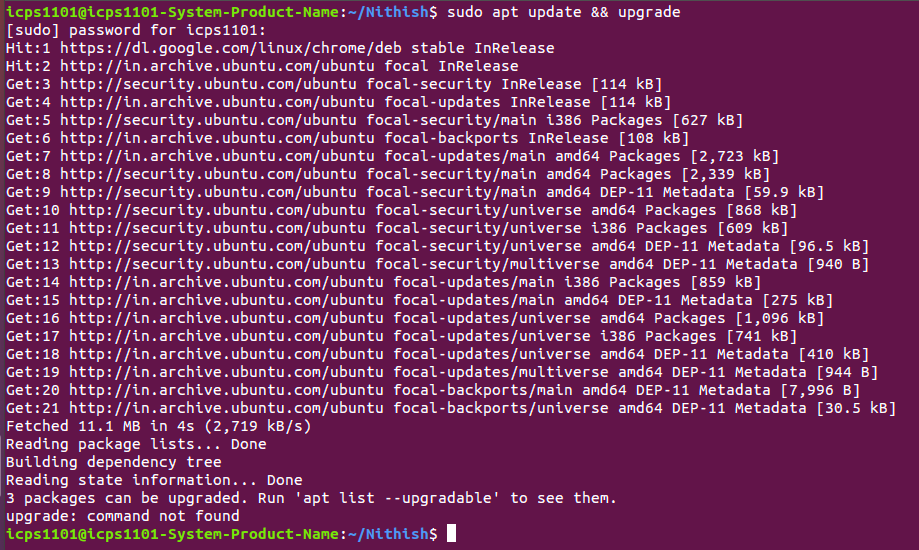
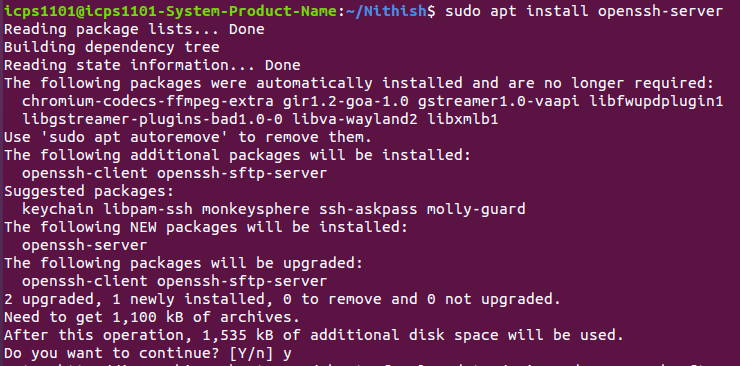
**Secure Shell (SSH)**

SSH is a cryptographic network protocol that allows secure remote access to a computer or server over an unsecured network. It provides a command-line interface for logging into remote systems and executing commands

1) Update and upgrade the apt



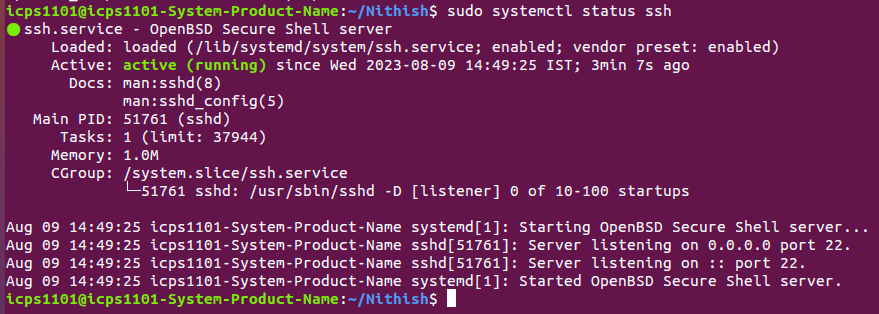
2) Install openssh server



3)Check the ssh version

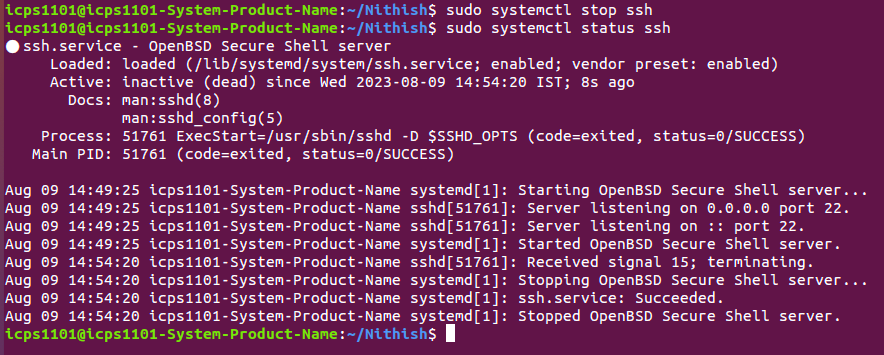


4) Once the installation is complete, the SSH service will start automatically. You can verify the status of SSH by using below command

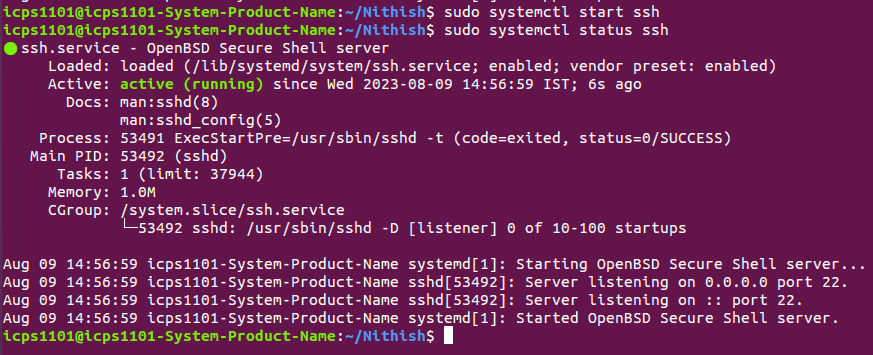


Press ‘q’ to get back to the command line prompt

5)if you want to make the ssh inactive, then use the below command



6) If you want to start the ssh again use the below command



Note : To do SSH, Make sure that the host system and remote system both installed with SSH and should be in active state.

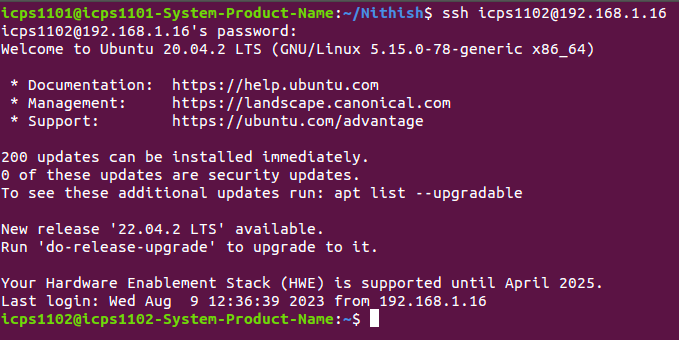
7) To login to remote system using SSH, you need

remote system’s ip-address,

username and

password

Now connect to your remote system via SSH, like below

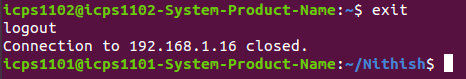


In the above image you can see the

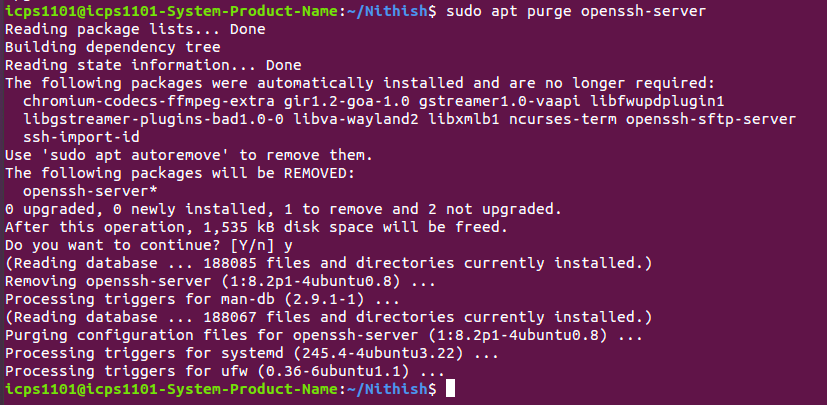
remote system name - icps1102

remote system address - 192.168.1.16

8) To logout from remote system



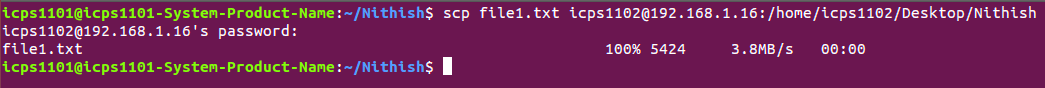
9) If you want to remove SSH from any system , use the following command



**Secure Copy(SCP)**

SCP uses the SSH protocol to securely transfer files between a local and a remote host. It provides a way to copy files and directories from one system to another

1) use the below command to copy a file from local to remote host



In the above image you can see the

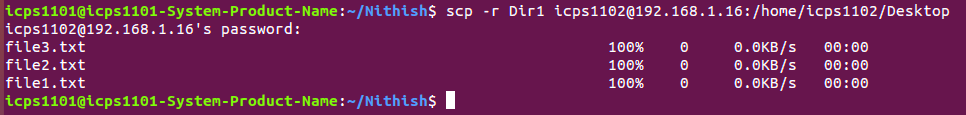
source - file1.txt

remote system user name - icps1102

remote system address - 192.168.1.16

destination path – home/icps1102/

2) To copy a directory from local host to remote host, use below command



**-r** is used for copying the **directories**

3) To copy all the directories and files within a directory, use below command

