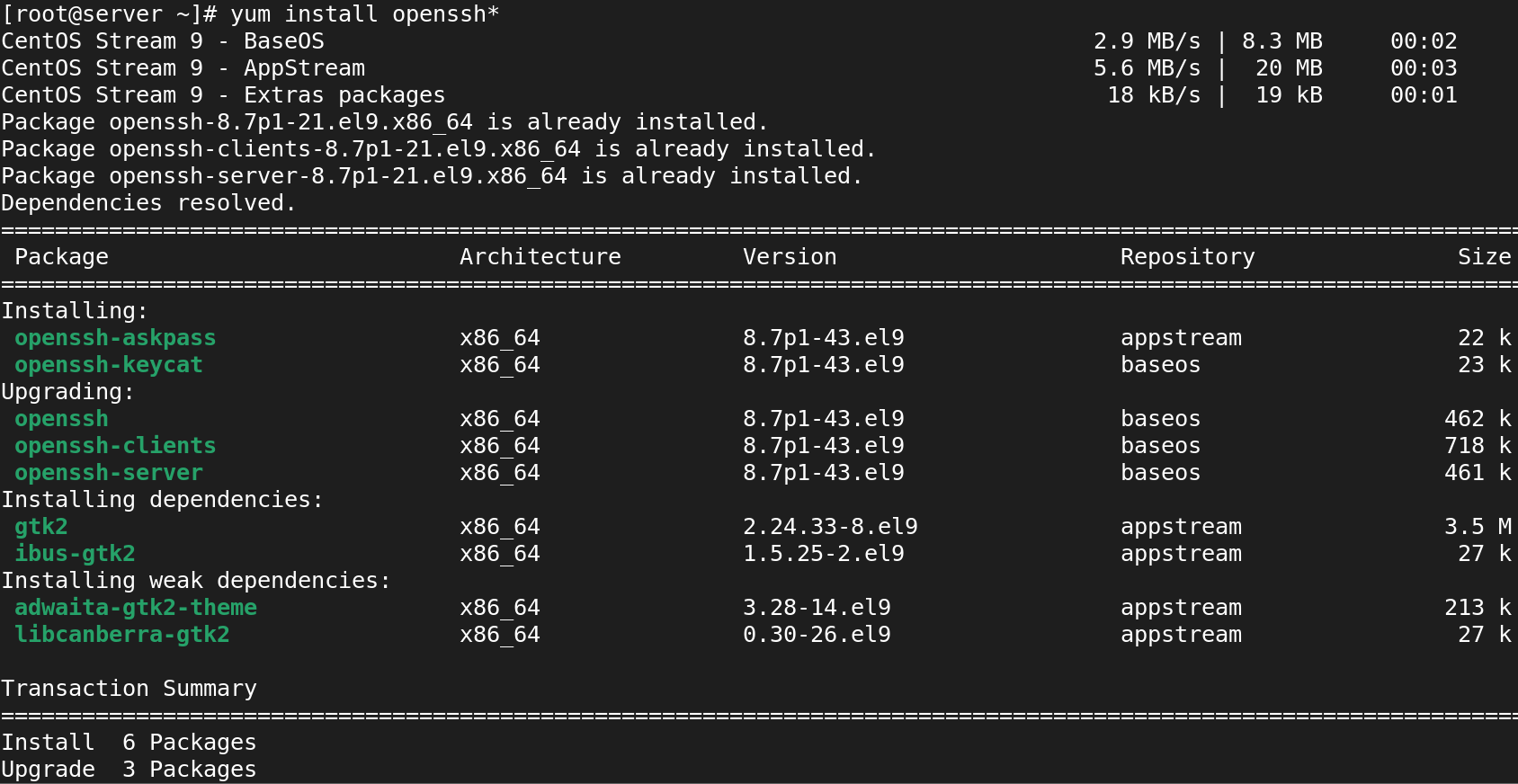
***Ssh***

*First step to change the host name*



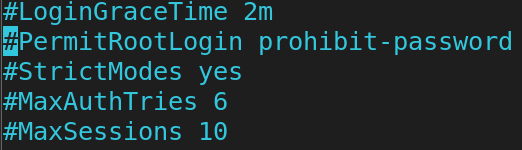


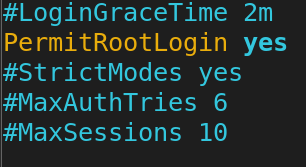
*Install open ssh for both server & client by using command yum.*



*Now we should login the client into the server side for that we should use further configuration in server side*





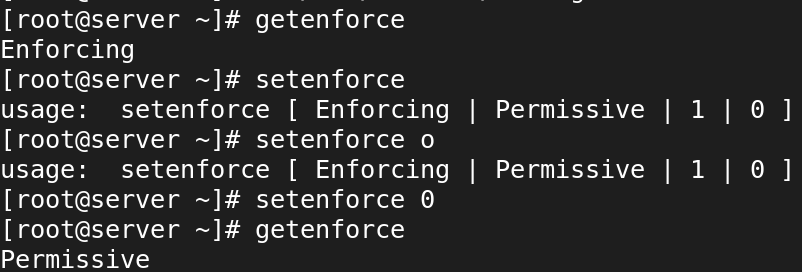


*Now we should diabled the selinux*

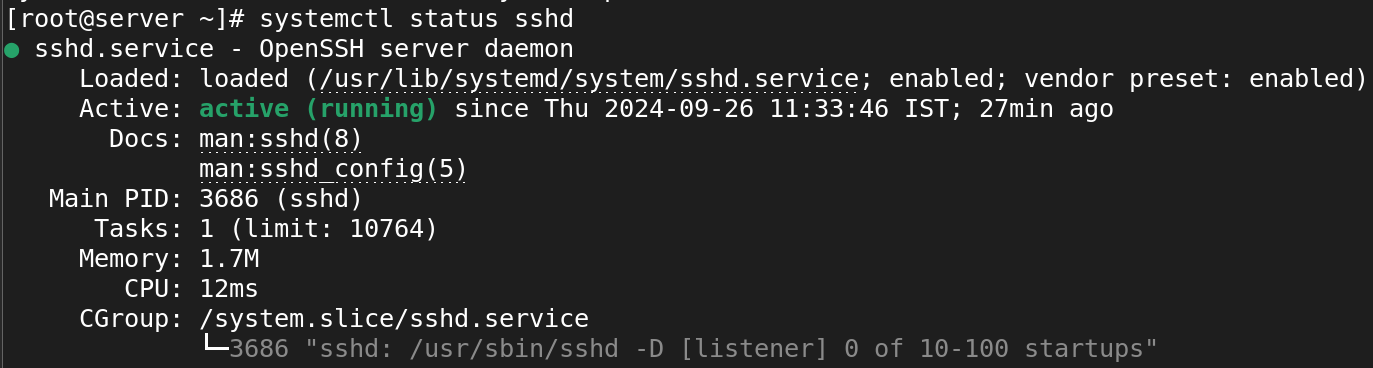




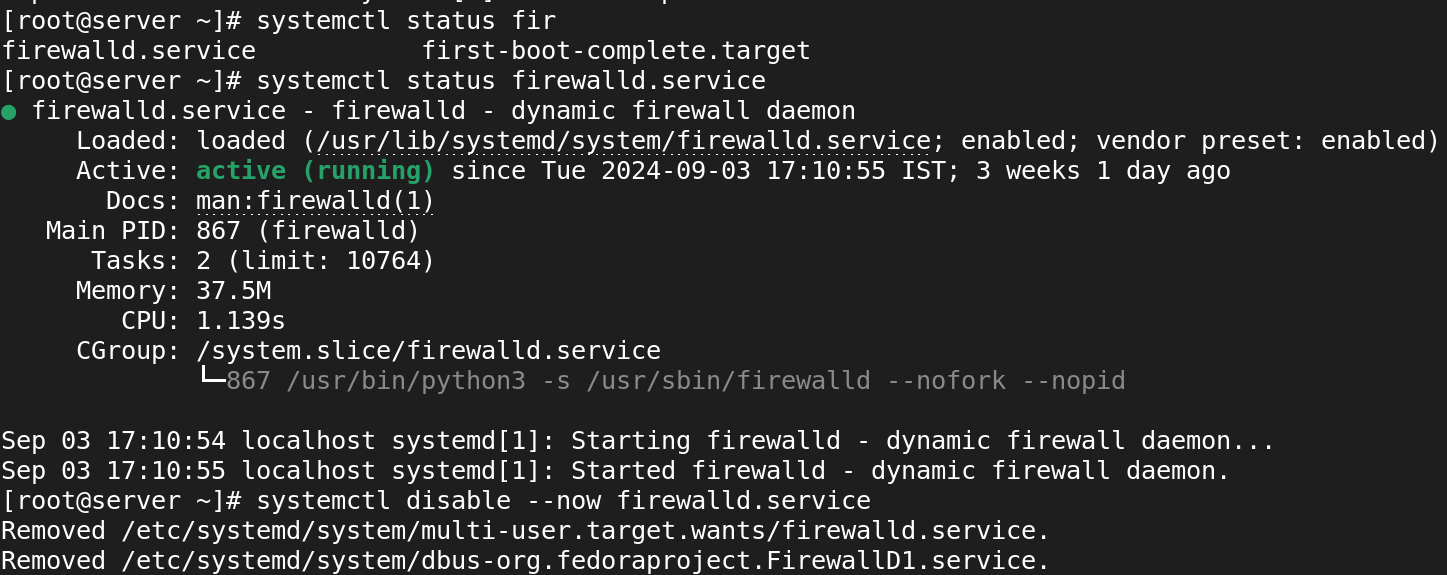




Now we use to see the status for sshd should be enable and active.

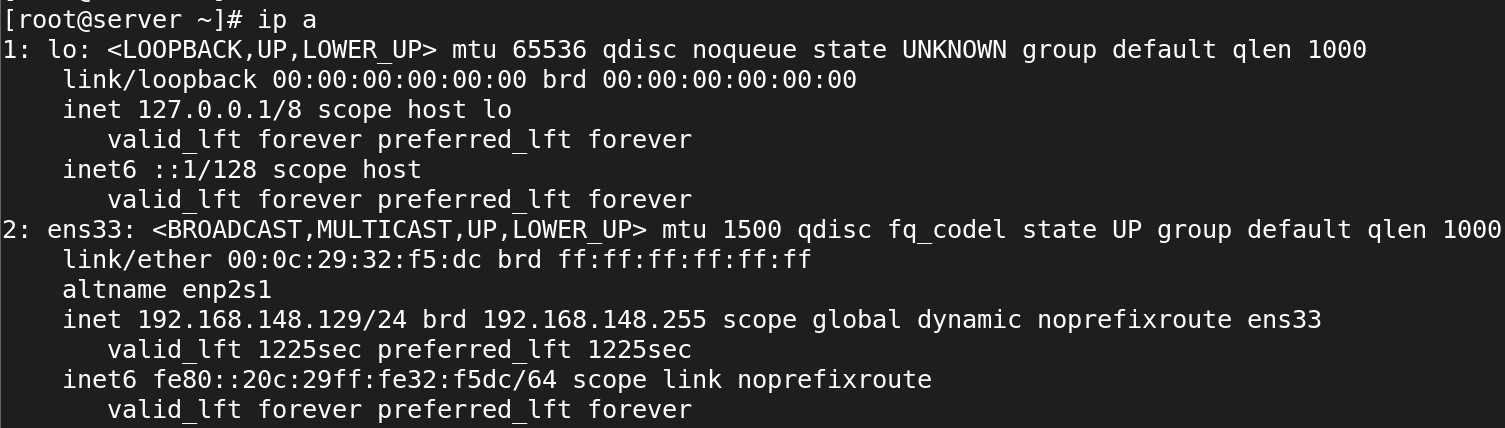


Now we use to see the status for firewalld and it should be disable and dead.

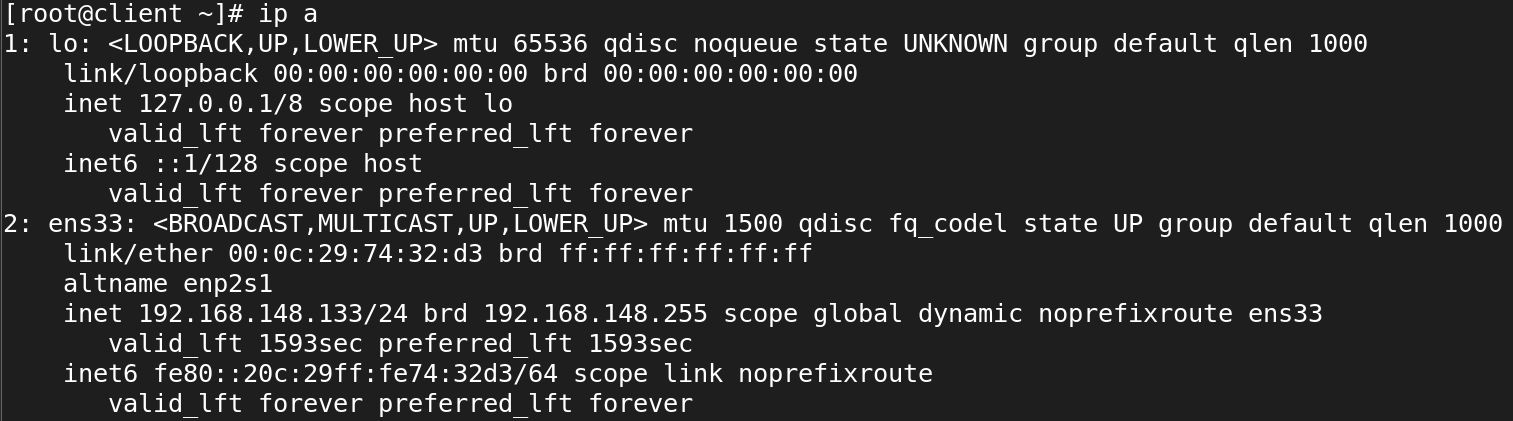


Now we should restart the service

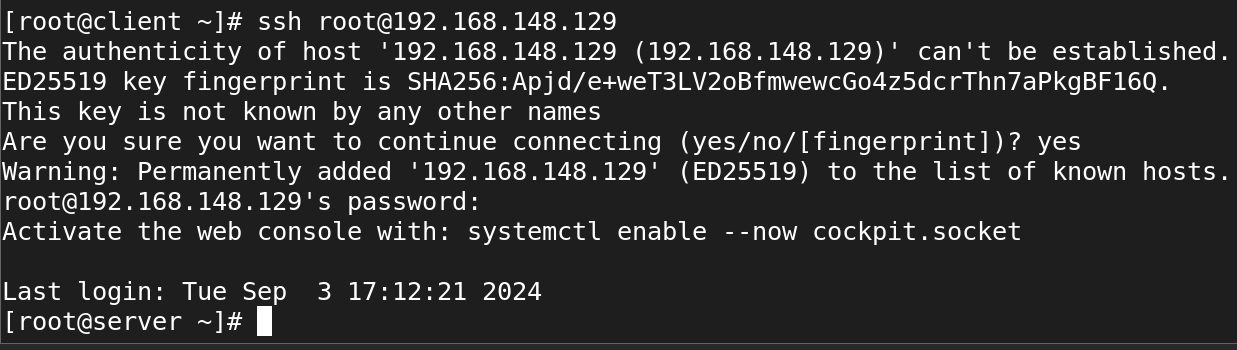




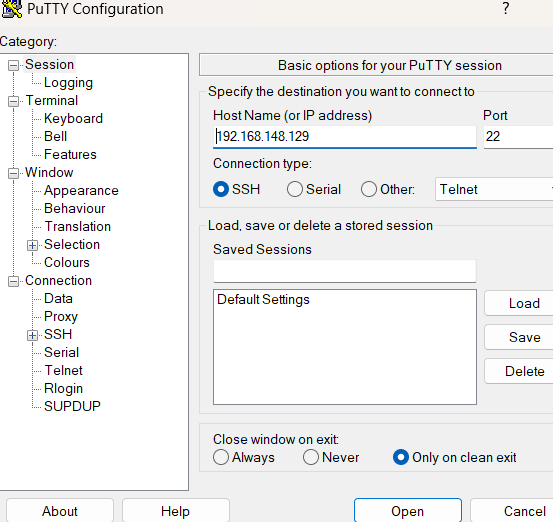
**ssh Client**

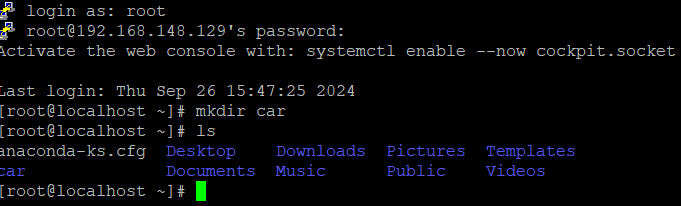


Now we use to login server from client side.



**Accessing in PUTTY**







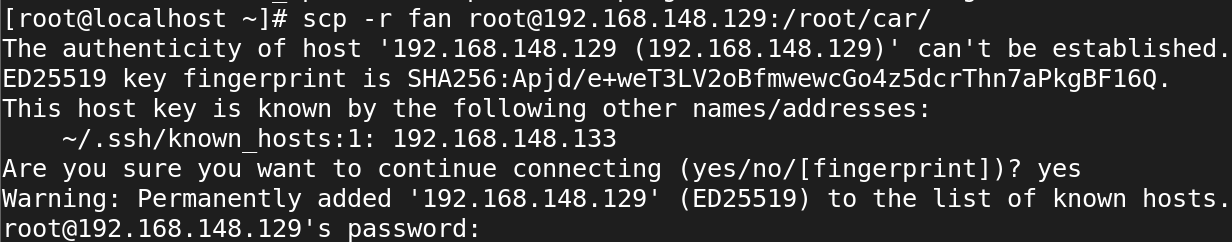
**Secure copy**

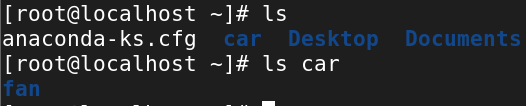
**copy file to remote server**

**#scp /root/securefile root@192.168.44.11:/tmp**

**copy directory to remote server**

**#scp -r /tmp/dir1 madhu@192.168.44.11:/home/madhu**





**Configure password-less SSH session (Key based authentication)**

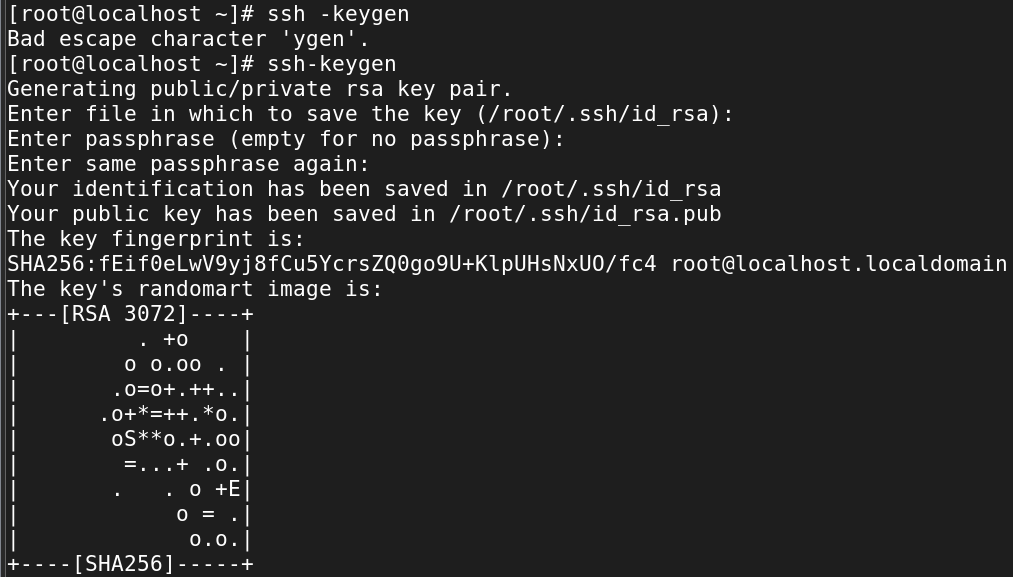
**Accessing server from client without password:**

**Generate public-private key pair**

**ssh-keygen**

**id\_rsa**

**id\_rsa.pub**



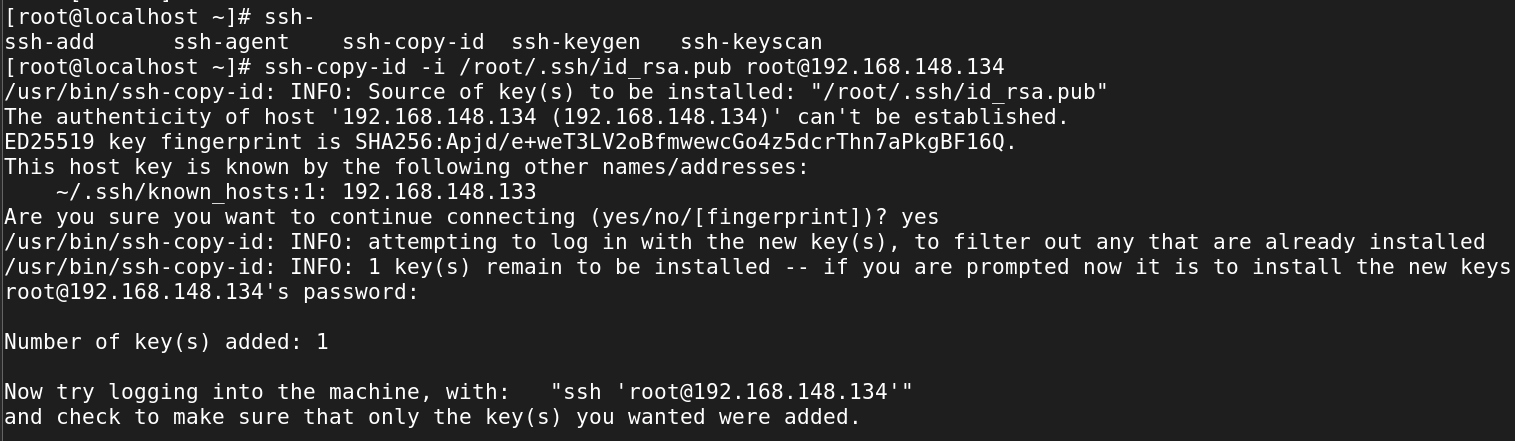
**Add public key to ~/.ssh/authorized\_keys file on remote host**

**ssh-copy-id -i ~/.ssh/id\_rsa.pub [root@192.168.119.128](mailto:root@192.168.119.128)**

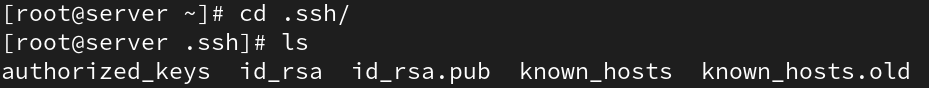
**-i option indicates identity file**

**~/.ssh/id\_rsa.pub is identity file**

**remaining text is remote user and remote server IP**



**Check the server file**

****

