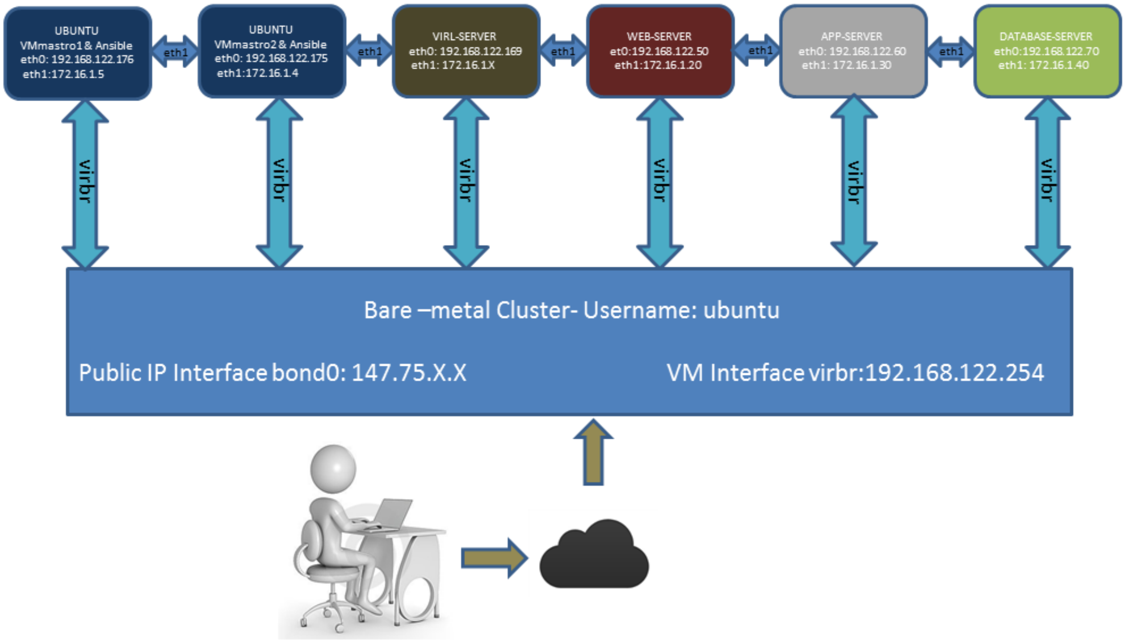
Ansible Network Automation Hands-on Exercises

Exercise-1: Understand test lab

Notes:

1. Please collect the Ansible Cluster IP address from Instructor before going forward
2. We will focus on Network Infrastructure simulation using VIRL in this document. Ansible network automation exercises will be dealt in other document.



Criterion SDCloud Platform is used for simulating the Ansible network automation Learning Lab. It consists of 5 components.

1. VIRL Server
2. VMM1 (VM Maestro Client and Ansible)
3. VMM2 (VM Maestro Client and Ansible)
4. Web server
5. App server
6. Database server

VIRL is Cisco's powerful network simulation platform. It has virtual machines running the same network operating systems as used in Cisco's physical routers and switches. It also has a user-friendly GUI for network design and simulation control.

VM Maestro is the GUI client used to communicate with VIRL server for creating topologies and to run simulations.

To access VM Maestro_1 to build a topology and run simulations:
VNC into the Ubuntu machine which has VMMaestro client installed on it using a VNC viewer by accessing public-ip-of-root-node:8888 using credentials **ubuntu/password**.
Similarly to access VM Maestro_2 to build topology and run simulations :
VNC into the Ubuntu machine which has VMMaestro client installed on it using a VNC viewer by accessing public-ip-of-root-node:9999 using credentials **ubuntu/password**

VMs and Credential's:

VM's	IP address	Username	Password	Domain
VMM1	eth0:192.168.122.176 eth1:172.16.1.5	ubuntu	Password	vmm1.local
VMM2	eth0:192.168.122.175 eth1:172.16.1.4	ubuntu	Password	vmm2.local
Web	eth0:192.168.122.50 eth1:172.16.1.20	web	Password	web.local
App	eth0:192.168.122.60 eth1:172.16.1.30	app	Password	app.local
db	eth0:192.168.122.70 eth1:172.16.1.40	db	Password	db.local
VIRL	eth0:192.168.122.169 eth1:172.168.1.X	ubuntu	Password	virl.local

Devices and credentials:

Devices	IP address	Username	Password	Domain
IosRouter1	Mgnt:172.16.1.151	cisco	cisco	router1.local
IosRouter2	Mgnt:172.16.1.152	cisco	cisco	router2.local
IosRouter3	Mgnt:172.16.1.153	cisco	cisco	router3.local
NxSwitch1	Mgnt:172.16.1.154	cisco	cisco	nxswitch1.local
NxSwitch2	Mgnt:172.16.1.155	cisco	cisco	nxswitch2.local

SSH Guide For different Operating System:

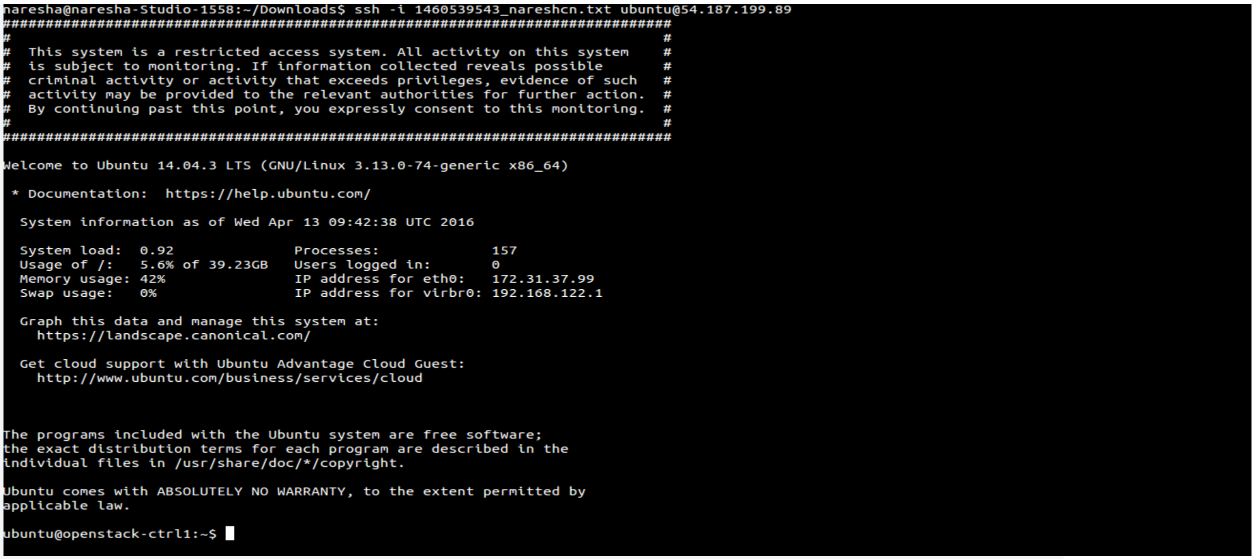
This helps to understand how to use SSH in different Operating Systems

For Linux & Mac Users*:*

Change the permission of the downloaded private key file like, *chmod 600 private_key_file.txt*

Access any node using ssh - i private_key_file.txt ubuntu@<ip of the node>

Example: *ssh - i 1460539289_nareshcn.txt ubuntu@54.200.239.38*

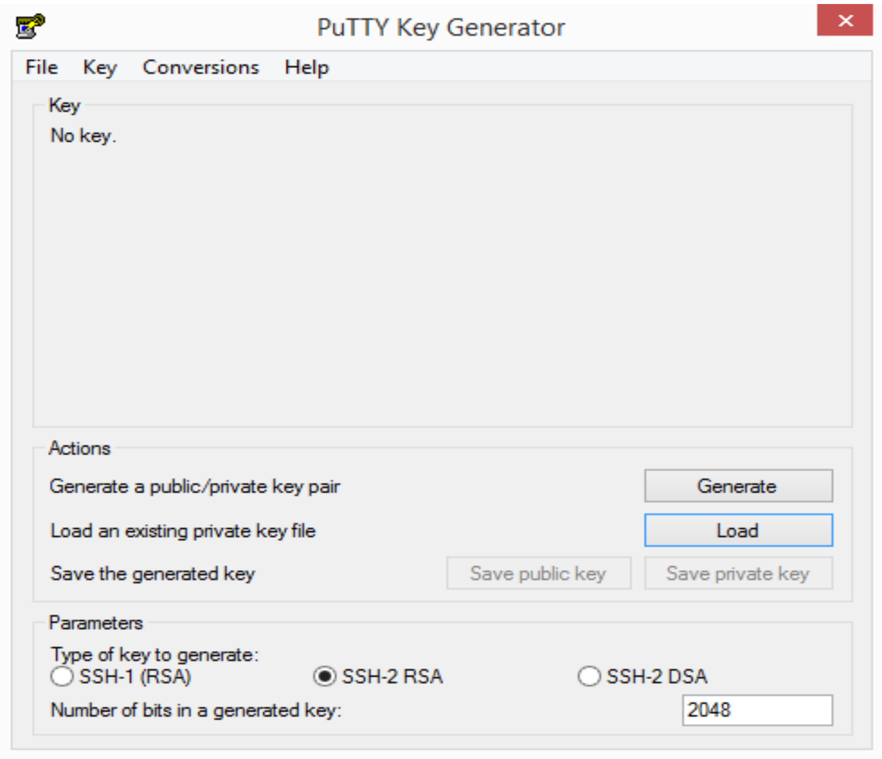


```
naresha@naresha-Studio-1558:~/Downloads$ ssh -i 1460539543_nareshcn.txt ubuntu@54.187.199.89
##############################################################################
#                                                                            #
#  This system is a restricted access system. All activity on this system    #
#  is subject to monitoring. If information collected reveals possible       #
#  criminal activity or activity that exceeds privileges, evidence of such   #
#  activity may be provided to the relevant authorities for further action.  #
#  By continuing past this point, you expressly consent to this monitoring.  #
#                                                                            #
##############################################################################

Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.13.0-74-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Apr 13 09:42:38 UTC 2016

  System load:  0.92              Processes:             157
  Usage of /:   5.6% of 39.23GB   Users logged in:       0
  Memory usage: 42%               IP address for eth0:   172.31.37.99
  Swap usage:   0%                IP address for virbr0: 192.168.122.1

  Graph this data and manage this system at:
    https://landscape.canonical.com/

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud



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.

ubuntu@openstack-ctrl1:~$ █
```

For Windows Users using an ssh client:

To login into the nodes using private key, you need an ssh client like PuTTY. You will also require PuTTYgen

(i).Ggenerate .ppk file from the text file downloaded before, using PuTTYgen.



Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

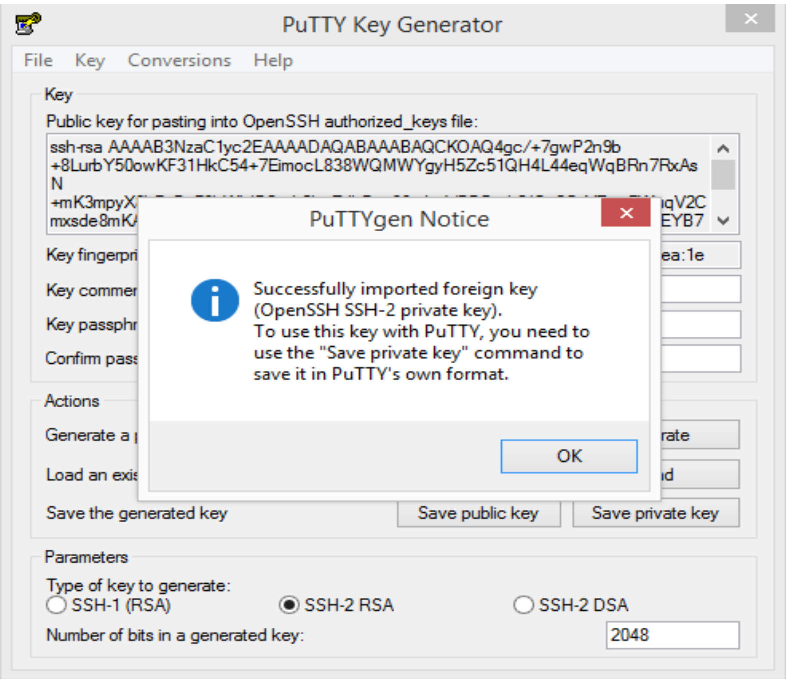
Parameters

Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

(ii).Load the downloaded key file which is in .txt format.



PuTTY Key Generator

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCKOAQ4gc/+7gwP2n9b
+8LurbY50owKF31HkC54+7EimocL838WQMWYgyH5Zc51QH4L44eqWqBRn7RxAs
N
+mK3mpyX                                              qV2C
mxsde8mK                                              EYB7
```

Key fingerpri ea:1e

PuTTYgen Notice

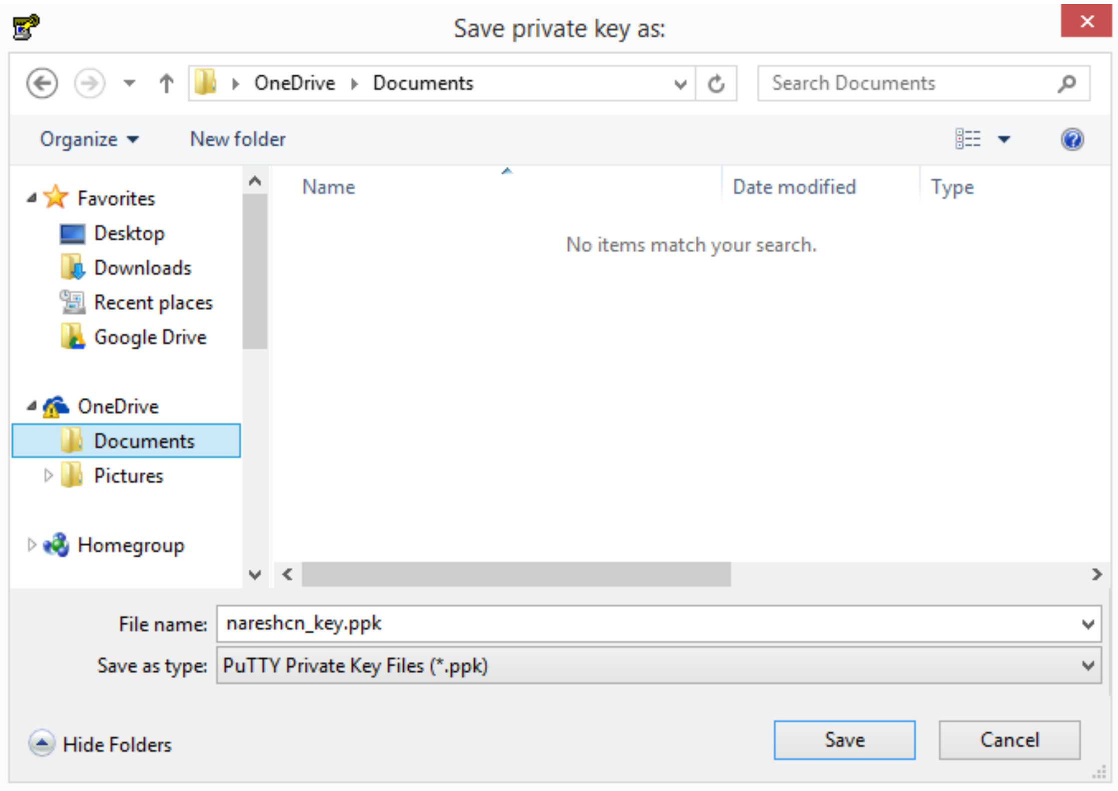
Successfully imported foreign key
(OpenSSH SSH-2 private key).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.

Parameters

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

(iii)Then save the private key in ppk format.



Save private key as:

OneDrive ▸ Documents

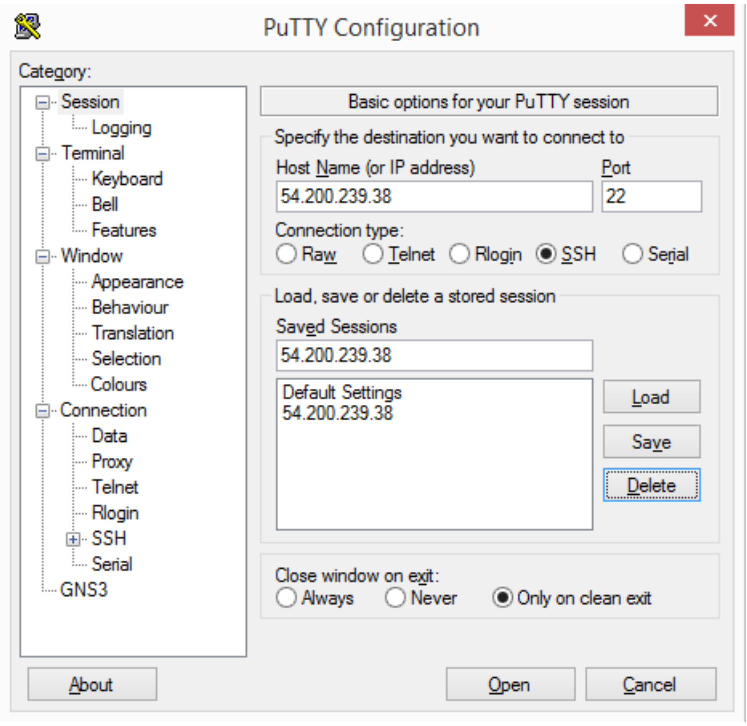
No items match your search.

File name: nareshcn_key.ppk

Save as type: PuTTY Private Key Files (*.ppk)

It is advisable not to enter pass phrase for the private key.

(iv)Using PuTTY create a session to login to nodes like,



Specify the destination you want to connect to

Host Name (or IP address): 54.200.239.38

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

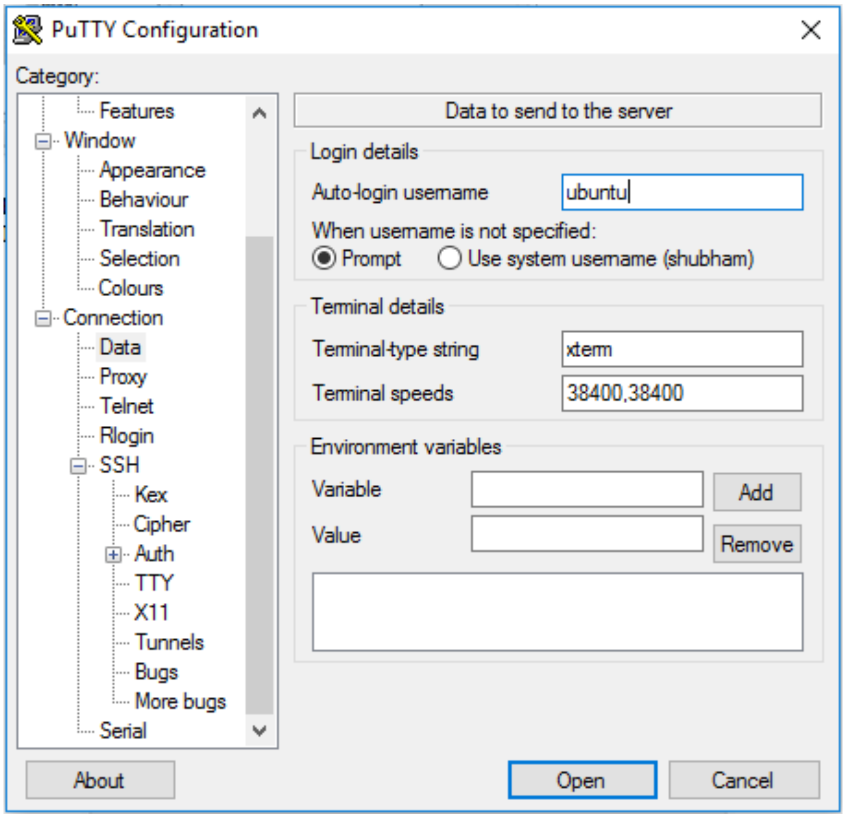
Saved Sessions: 54.200.239.38

Default Settings
54.200.239.38

Close window on exit: ○ Always ○ Never ● Only on clean exit

s

(v)Provide the IP address of the node in which you want to login. Save the session. Click on Data and enter Auto-Login Username as ‘ubuntu’.



Login details

Auto-login username: ubuntu

When username is not specified: ● Prompt ○ Use system username (shubham)

Terminal details

Terminal-type string: xterm

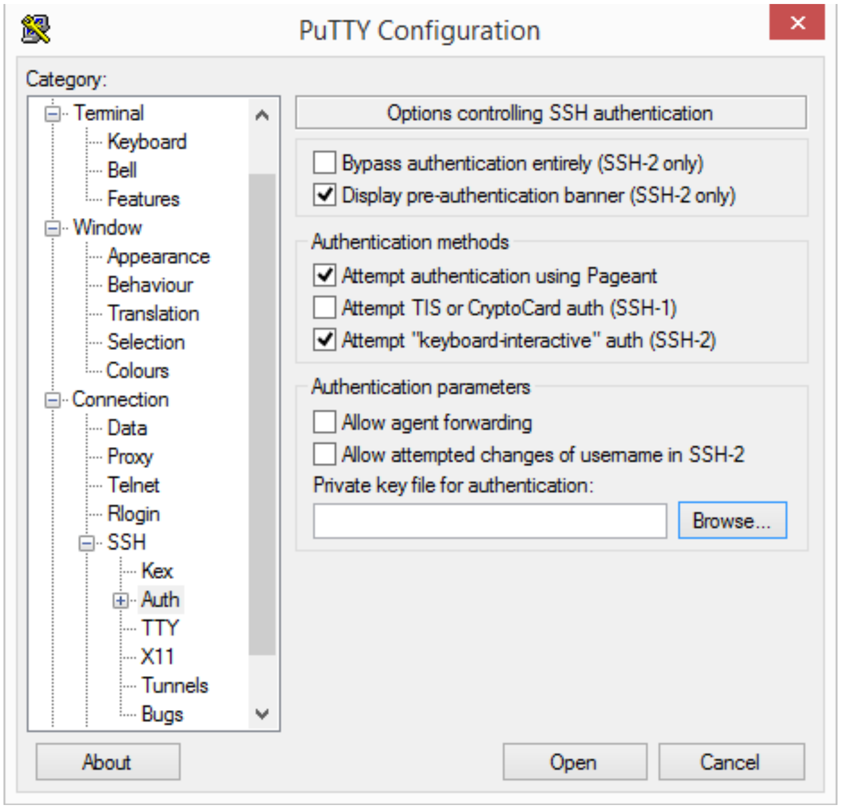
Terminal speeds: 38400,38400

Environment variables

Variable:

Value:

(vi)Click on Auth and select the private key you just generated using PuTTYgen tool.



PuTTY Configuration

Options controlling SSH authentication

☐ Bypass authentication entirely (SSH-2 only)
☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

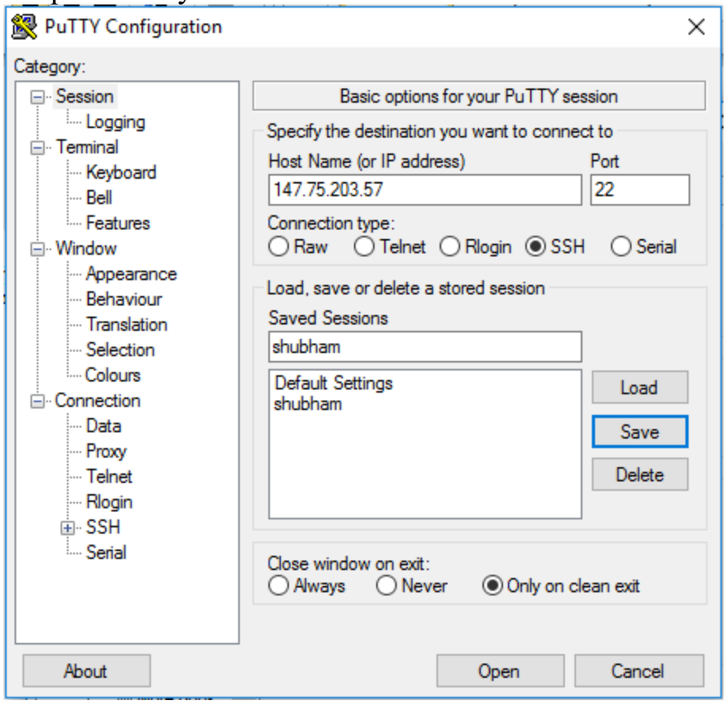
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

(vii)Then click Session on save the session again. Now you can login to your node with the private key.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 147.75.203.57
Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: shubham

Default Settings
shubham

Close window on exit:
○ Always ○ Never ● Only on clean exit