

IST198

OpenStack

Administration

Version 1: 2017-08-16

These exercises will guide the student through the concepts and topics learned in chapter 6, manage key pairs and connect to an instance using PuTTY and a key pair in OpenStack Mitaka installed on CentOS 7.

Manage Key Pairs and Connect to an Instance using a Key Pair.



This material is based upon work supported by the National Science Foundation under Grant No. (NSF 1601166). This work was created by Ron Sharman of Trident Technical College and is licensed under the Creative Commons Attribution 4.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Attributions:



This material is based upon work supported by the National Science Foundation under Grant No. (NSF 1601166).



openstack®

Portions of this document, in whole or part, were sourced from the OpenStack website at <https://OpenStack.org>



Contents

Attributes	1
Contents	2
Introduction	3
Lab Objectives	4
Prepare the OpenStack virtual machines	5
Lab Scenario and Settings	6
Run the Lab setup script	8
Access the OpenStack Dashboard	12
Lab 14: Manage Key Pairs	16
Lab 15: Connect to an Instance using PuTTY on Windows	39
Lab 16: Connect to an Instance using the command line on Linux	48
Run the Lab grade script	59
Conclusion	63



Introduction

You have been hired as an intern with CLOUDTech Inc. CLOUDTech is a Cloud Computing consulting firm and Cloud Provider supporting thousands of clients in the region. The company provides a wide range of services to support migrating client Information Technology infrastructure to a Private, Hybrid or Public Cloud environment. You learned that the company has multiple departments and you will start your internship working with the Cloud hosting department customer support team.

The Cloud hosting department provides multiple platform and vendor Cloud hosting services for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and many other as a service offerings. The support team is responsible for helping customers with any issues related to their Cloud infrastructure hosted at and provided by CLOUDTech.

You will perform hands-on exercises to learn about the OpenStack Cloud implementation CLOUDTech uses to host customer Cloud environments.



Lab Objectives

Learner will be able to:

- Manage OpenStack Key Pairs, SSH to an instance using PuTTY installed on a Windows VM and SSH to an instance using the Linux command line

Labs 14-16

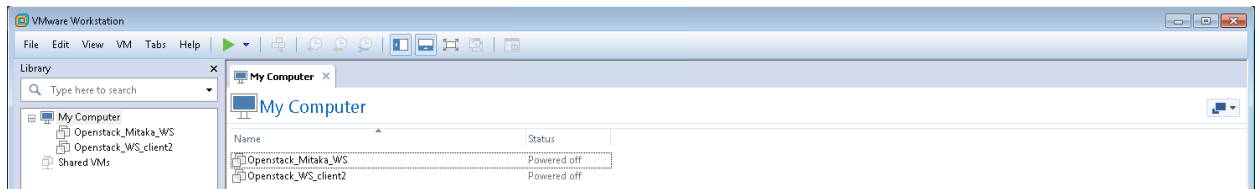
This lab will guide the student through managing OpenStack Key Pairs, connecting to an instance using PuTTY and the Linux command line.

(Note: This lab is designed to be completed on an NDG NETLAB System with the IST198_OpenStack_HXXX POD installed. The labs can also be completed on a physical machine with the appropriate software packages installed, or a PC that has VMware Workstation installed with the appropriate virtual machines configured).

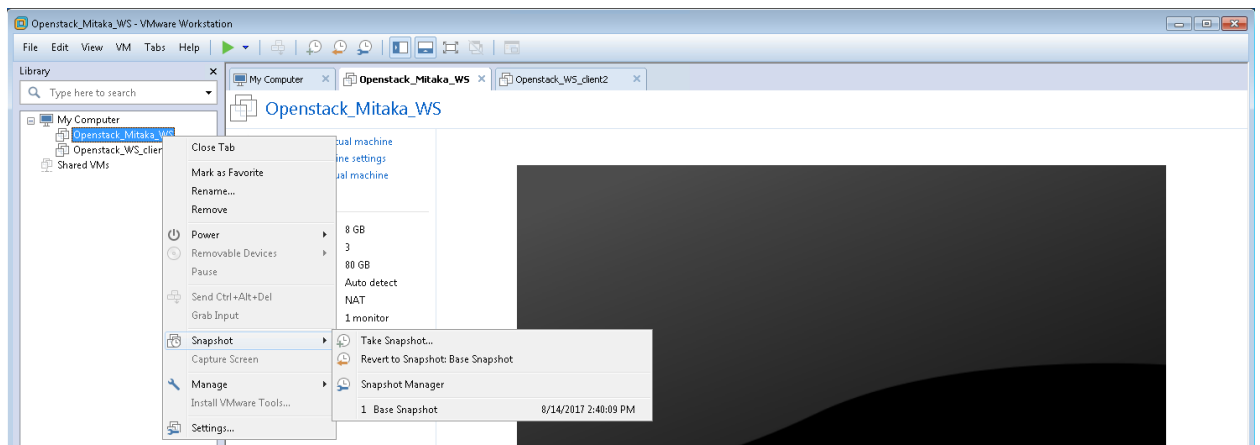
Prepare the OpenStack Virtual Machines



1. **Launch the VMware Workstation Pro application**

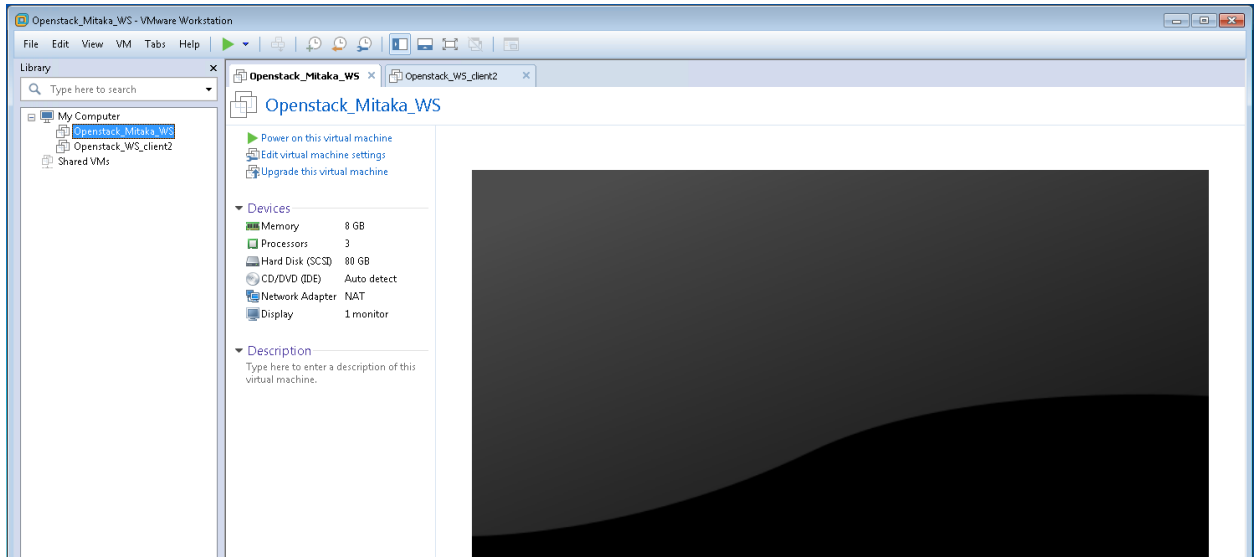


2. Workstation should have two virtual machines (VM) installed; Openstack_Mitaka_WS and Openstack_WS_client2.



3. Ensure that the Openstack_Mitaka_WS is at the correct starting point by reverting to the base snapshot. Right Click on Openstack_Mitaka_WS then Snapshot>Base Snapshot. Repeat for the Openstack_WS_client2 VM.

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



4. **Power on** both VMs by selecting one of the two VMs and **clicking on Power on this virtual machine**. Repeat for the other VM.

Lab Scenario

As part of CLOUDTech's customer support team, this is your third field visit to XYZ Company. During this visit, you will assist the customer with managing their key pairs and using the key pair to connect to their instance using Putty and the Linux command line.

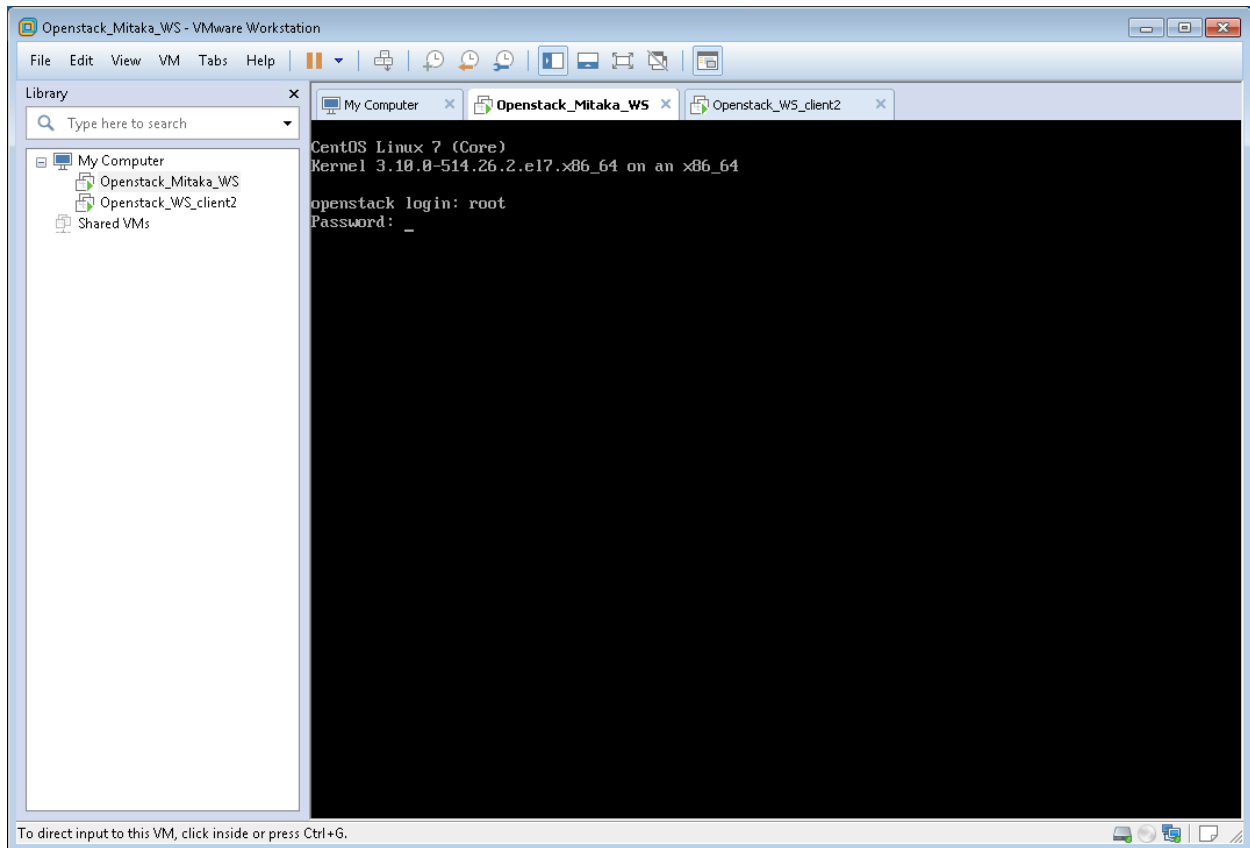
Lab Settings

The information in the table below will be needed in order to complete the labs. The task sections that follow provide details on the use of this information

Virtual Machine (VM)	IP ADDRESS	Account	Password	VM Type
Client2	10.220.0.2	Student	P@ssword	CentOS 7 Client
Server1	10.220.0.30	root	P@ssword	OpenStack Mitaka
OpenStack Dashboard	10.220.0.30	Student	P@ssword	Web Page Login credentials

Note: In this OpenStack VMware Workstation environment, the two VMs can be reverted back to their base snapshot at any time. This means that you can explore or experiment without fear of permanently damaging the OpenStack environment. If you make a mistake that you can't recover from, then stop and revert the appropriate VM to the base snapshot and everything will be back to a known good starting point.

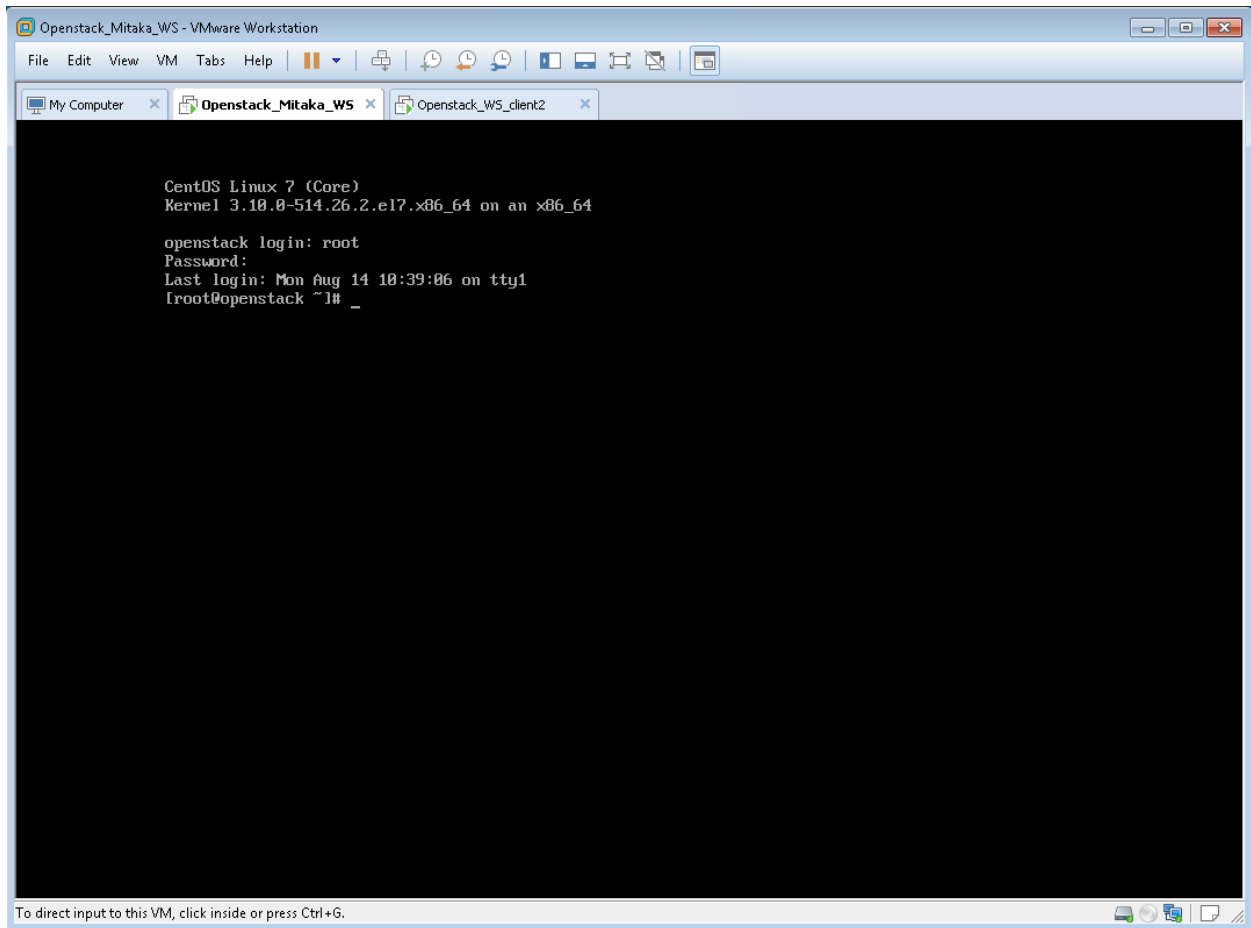
Run the lab setup script



1. Log in as **root** with the Password: **P@ssword**

Note: The password is NOT visible as you type it

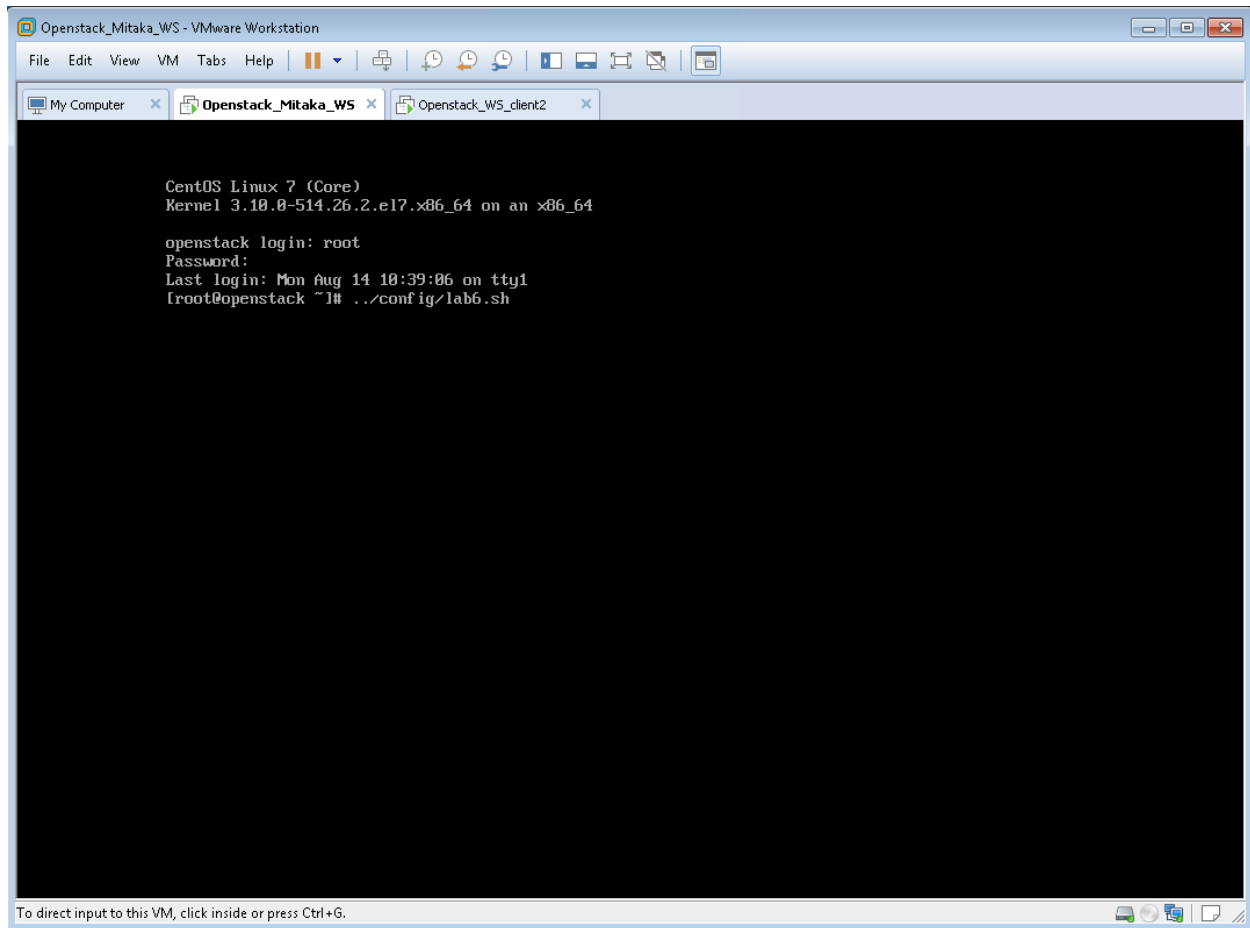
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



2. After successfully logging in as root, you should see this screen. Continue to the next page



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



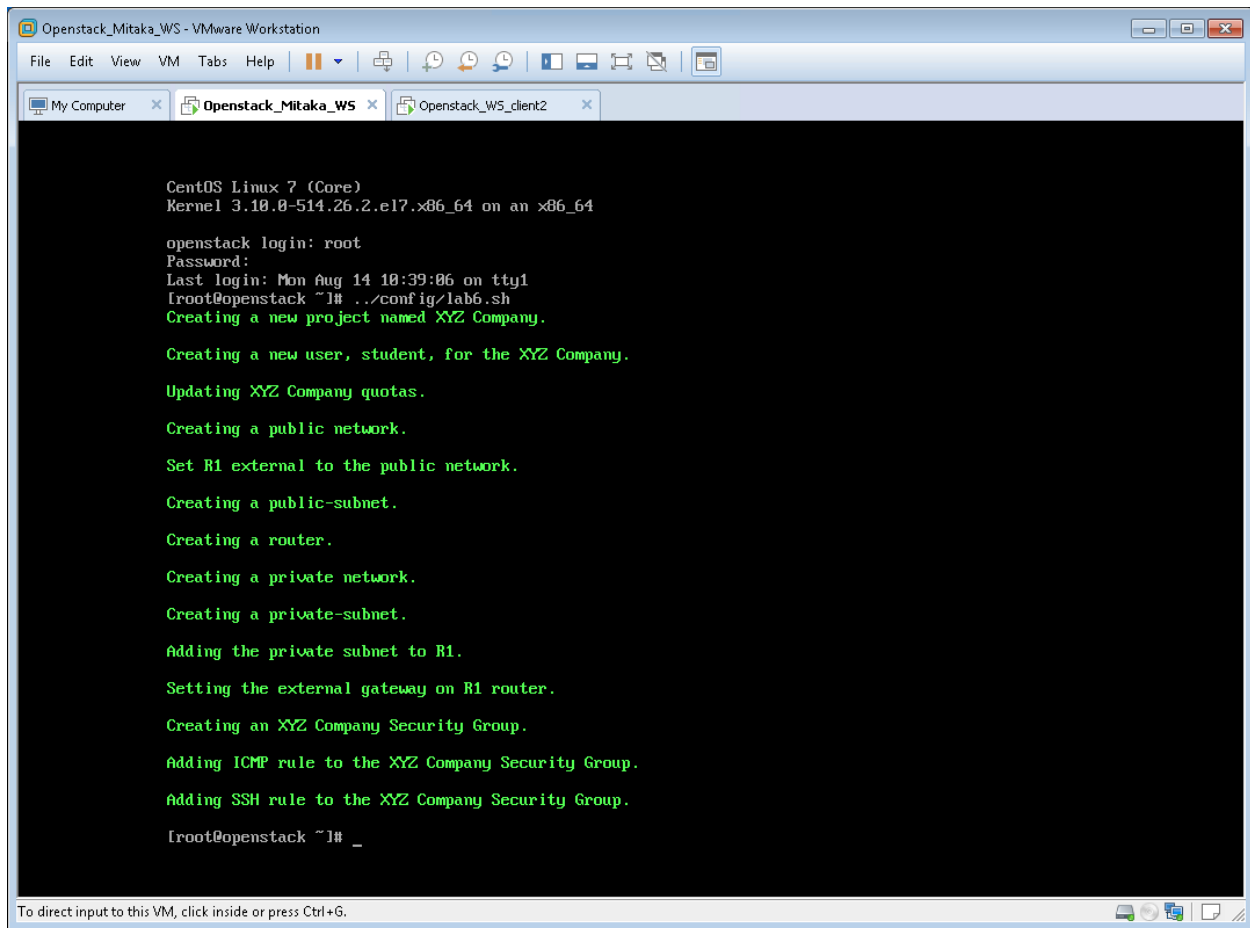
```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.2.el7.x86_64 on an x86_64

openstack login: root
Password:
Last login: Mon Aug 14 10:39:06 on tty1
[root@openstack ~]# ./config/lab6.sh
```

3. Type the command; **../config/lab6.sh** and **press Enter** as shown in the screen capture above to run the Lab 6 setup script



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.2.el7.x86_64 on an x86_64

openstack login: root
Password:
Last login: Mon Aug 14 10:39:06 on tty1
[root@openstack ~]# ./config/lab6.sh
Creating a new project named XYZ Company.

Creating a new user, student, for the XYZ Company.

Updating XYZ Company quotas.

Creating a public network.

Set R1 external to the public network.

Creating a public-subnet.

Creating a router.

Creating a private network.

Creating a private-subnet.

Adding the private subnet to R1.

Setting the external gateway on R1 router.

Creating an XYZ Company Security Group.

Adding ICMP rule to the XYZ Company Security Group.

Adding SSH rule to the XYZ Company Security Group.

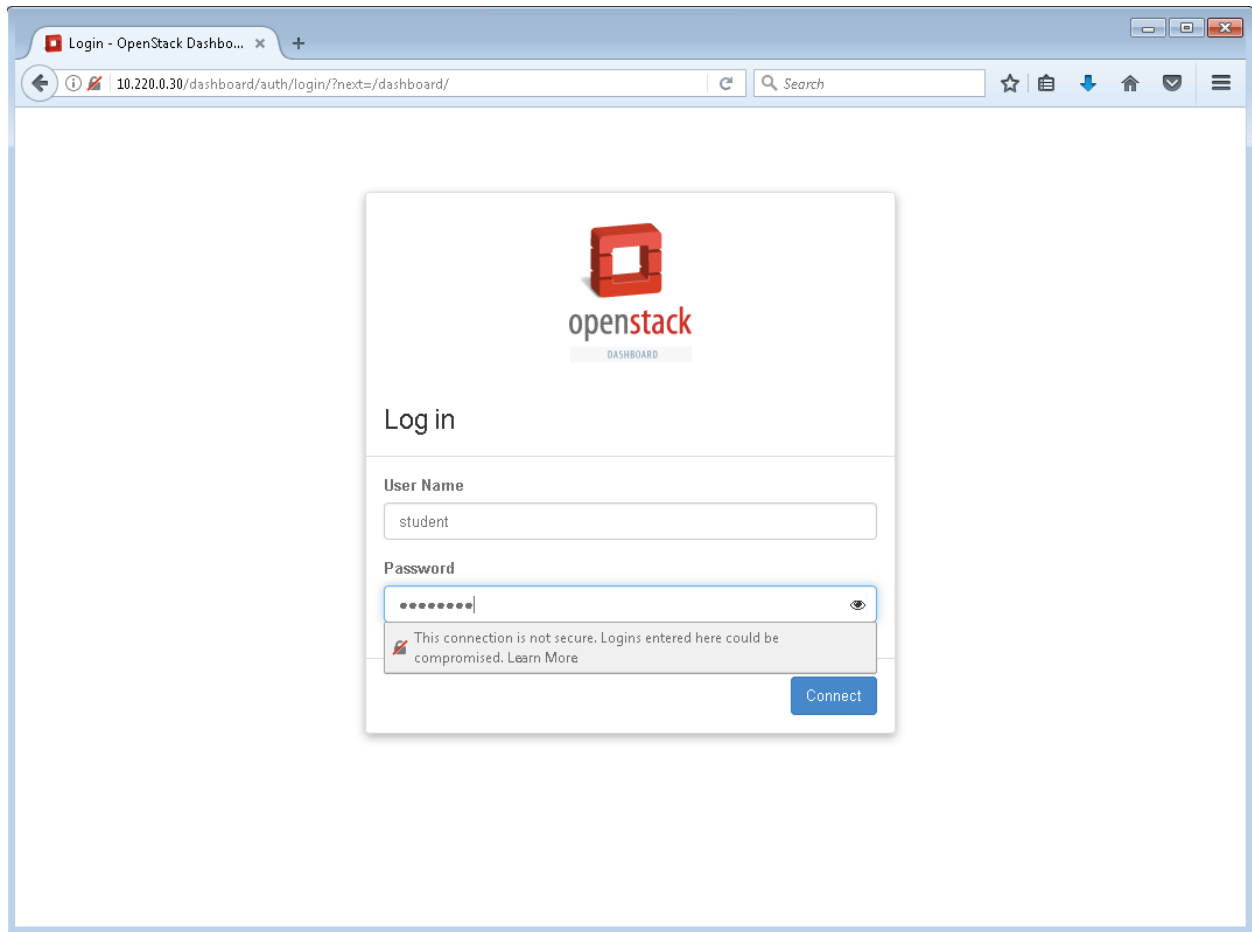
[root@openstack ~]# _
```

4. After the setup command completes, you can **minimize VMware Workstation**.

Note: The script is complete when the **[root@openstack ~]#** prompt returns



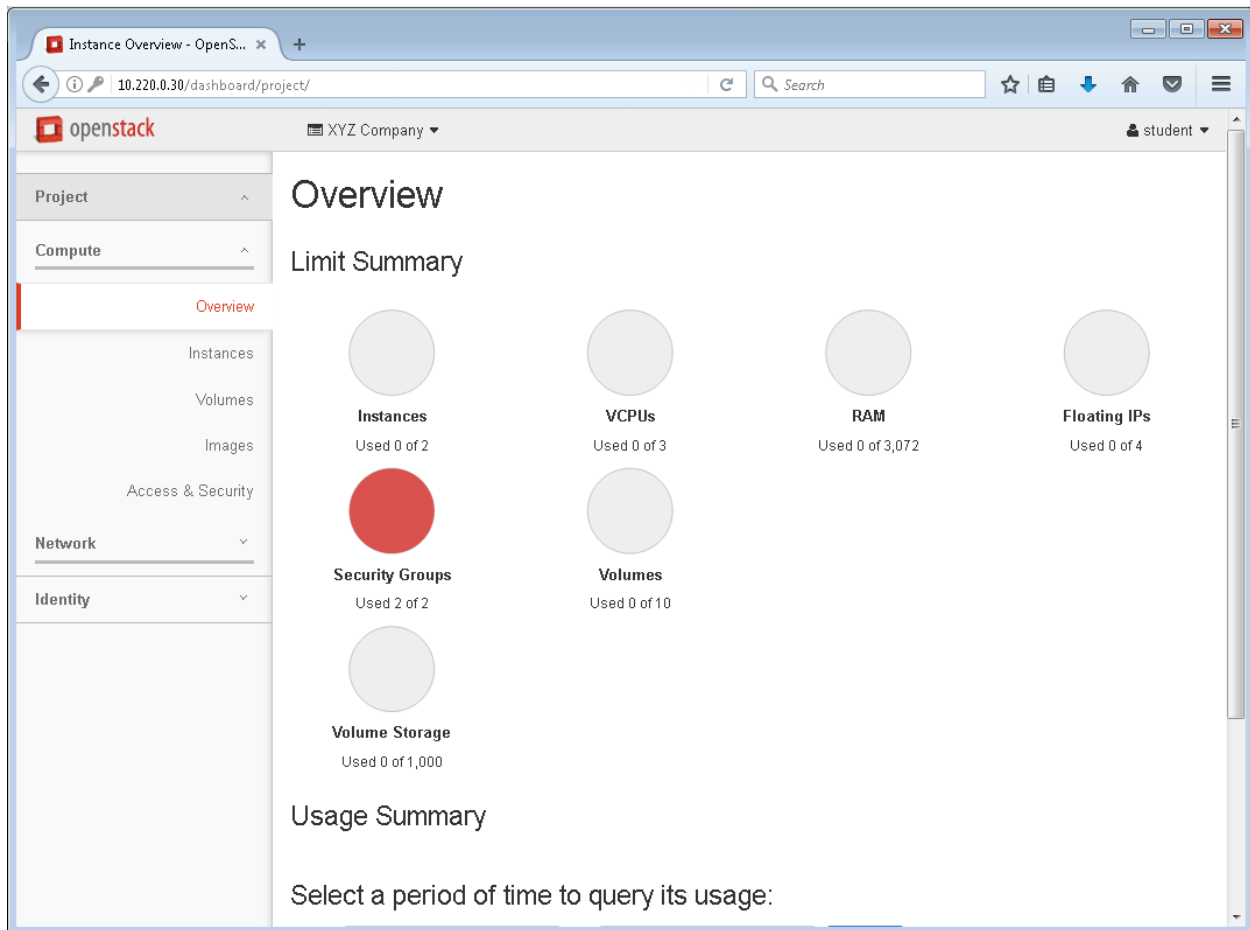
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



2. **Navigate** to **http://10.220.0.30/dashboard**. **Login** to the OpenStack Dashboard with the username **student** and **P@ssword** and press **enter** or **click Connect**

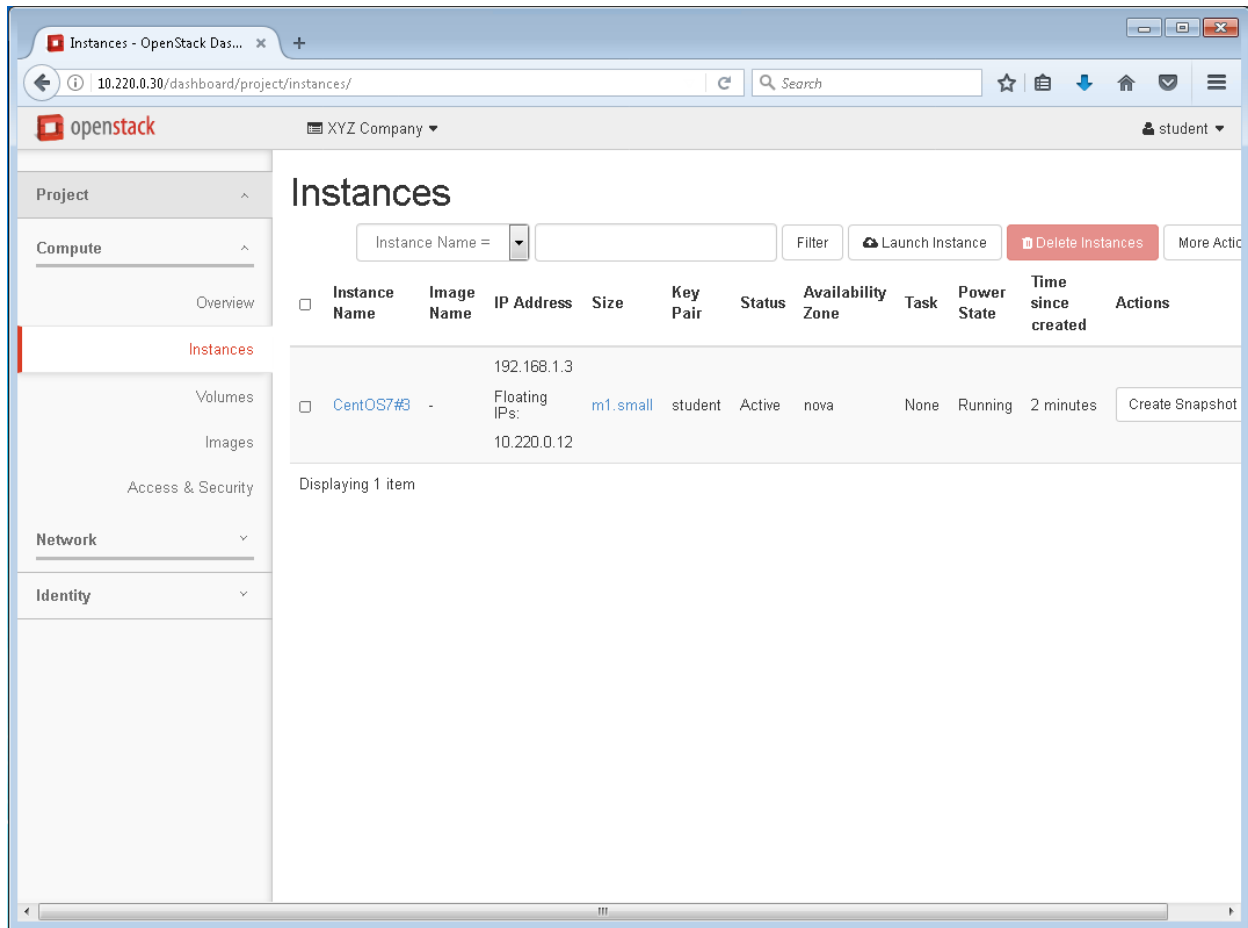
Note: User Name entries are not case sensitive, passwords are.

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



5. This is the homepage of the OpenStack Dashboard as seen from the XYZ Companies' customer perspective.

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



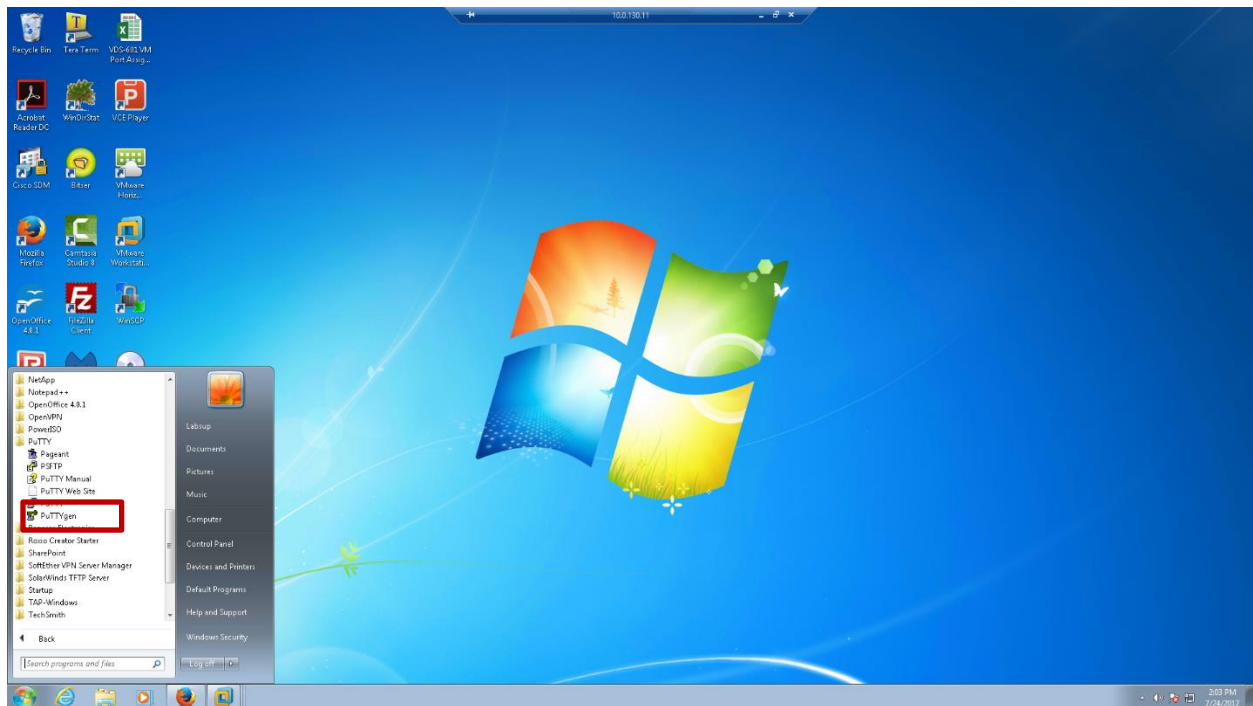
5. Using the techniques learned in previous labs, **upload the student key pair first**, and **then launch an instance** using the information in the table below.

Instance Name	CentOS7#3
Source	CentOS
Flavor	m1.small
Network	private
Security Groups	XYZ Company
Key Pair	student
Floating IP Address	10.220.0.12

Note: Why didn't we script this portion of lab 6? As a cloud user you would probably use the same key pair to access numerous instances, so you would have to upload that key pair for any new instances that you are spawning. Additionally, there is not an easy solution to script the uploading of a file from one VM to another VM, and practicing your new skills is always a good thing. Refer to previous lab instructions as needed to complete the process.



Lab 14: Manage Key Pairs

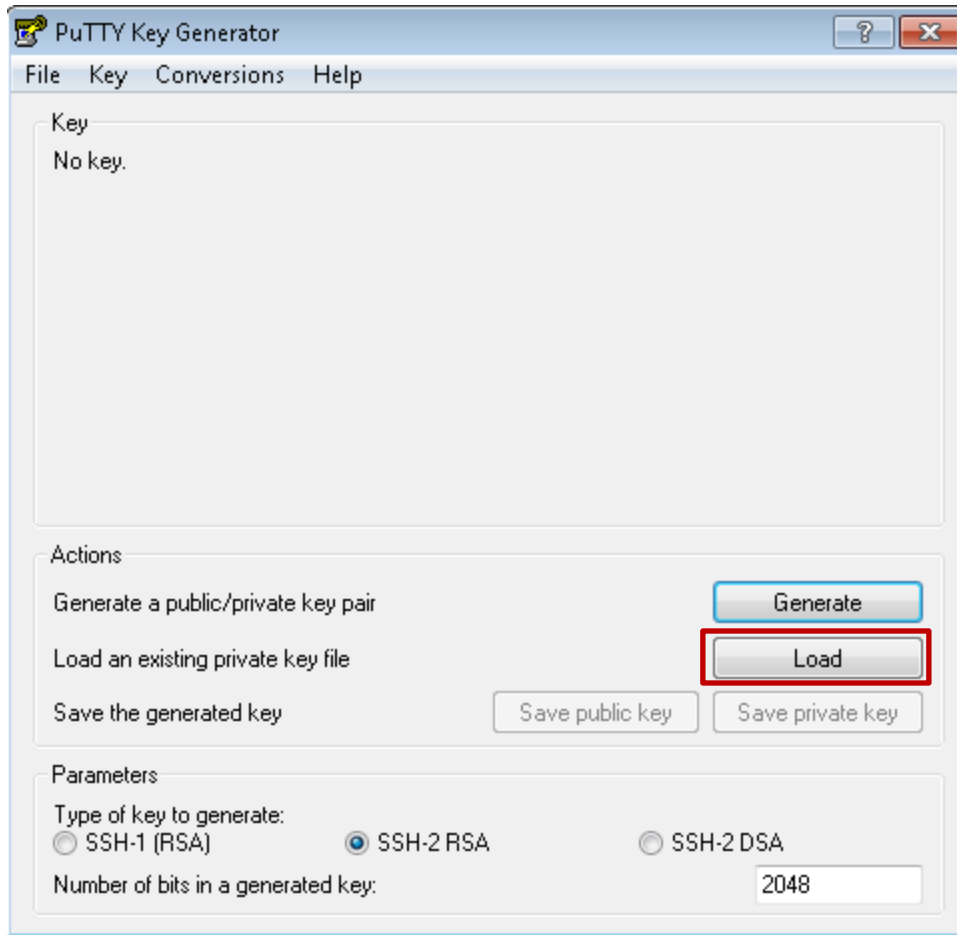


1. OpenStack Key Pairs will require different techniques depending on what Operating System (OS) that you are using. To connect to a Linux instance using the PuTTY terminal emulator on a Windows OS, the key pair must be converted to .ppk file first, this is because PuTTY is not compatible with the .pem OpenStack key pair format. On the Windows host **open PuTTYgen**

Note: PuTTY, PuTTYgen and WinSCP are all free downloads.

Key Pairs

Key pairs enable SSH access to an instance. The key pair is injected into the instance as the instance is launched. The image used to create instance must contain the cloud-init package.

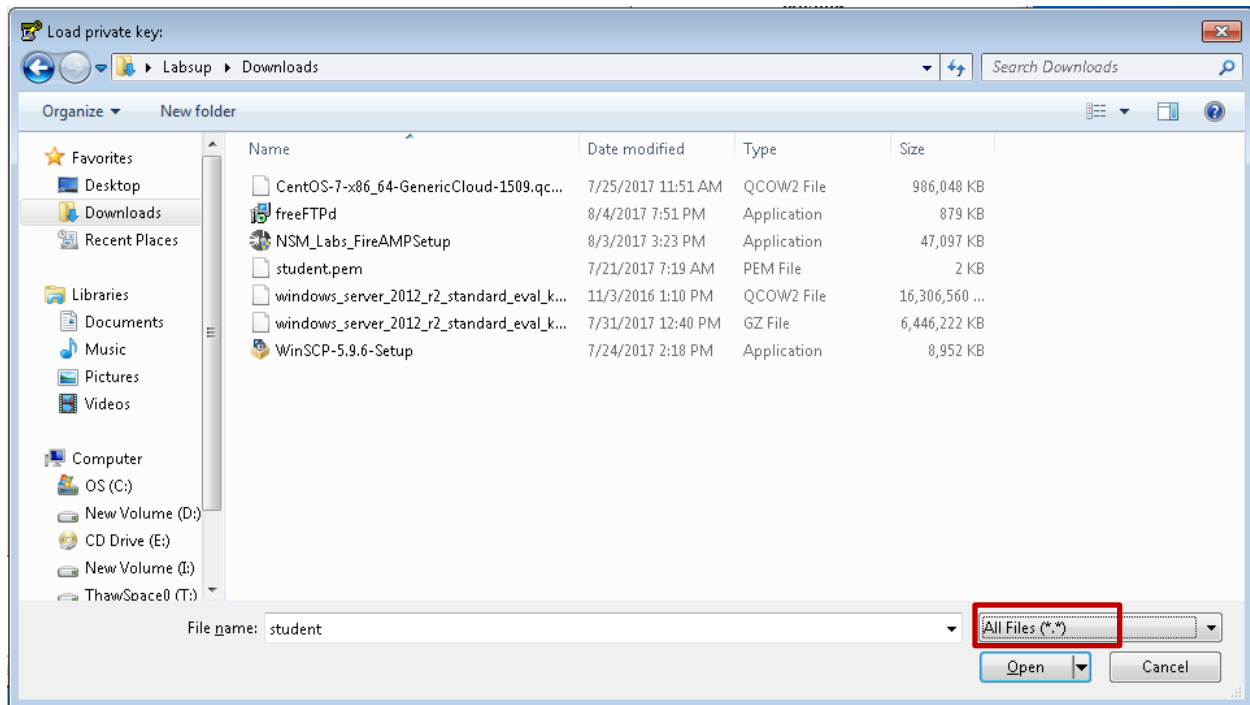


2. Once the PuTTY Key Generator opens, **Click on Load**

Key Pairs

Key pairs belong to an individual, not a project. To share a key pair across multiple users, each user needs to import that key pair.

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



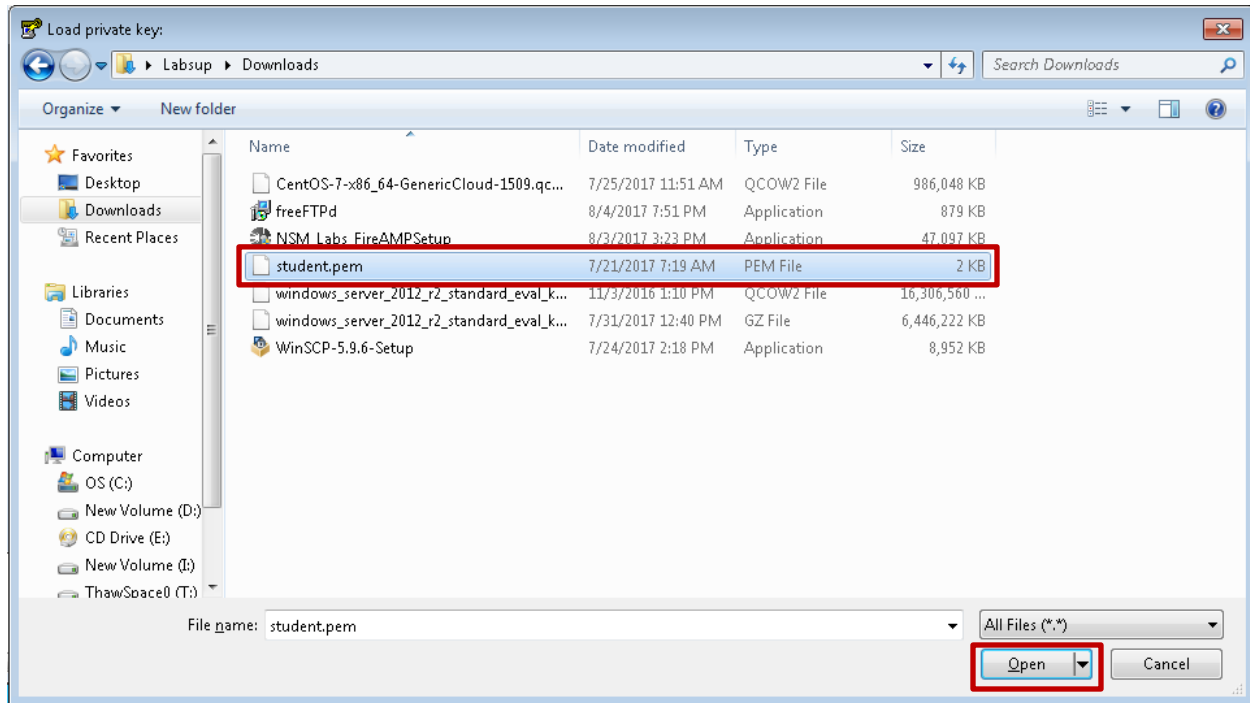
3. Navigate to the Downloads folder, and using the dropdown menu, select All Files (*.*)

Note: This lab assumes that the Key Pair that was created in a previous lab is still in the Downloads folder. If not, create another key pair and save it to the Downloads folder and proceed with the lab.

Key Pairs

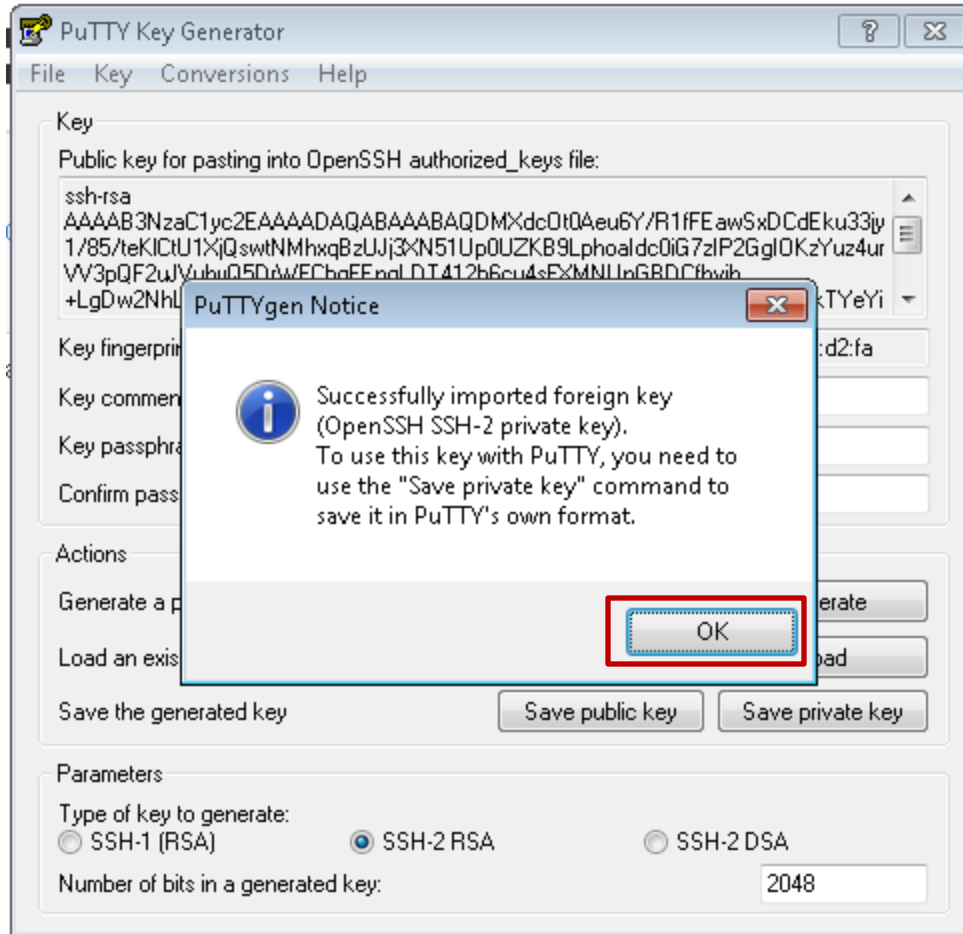
If an instance was created with a key pair injected, then you cannot access that instance without the that key pair.

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



4. Select the **student.pem** file and Click on **Open**

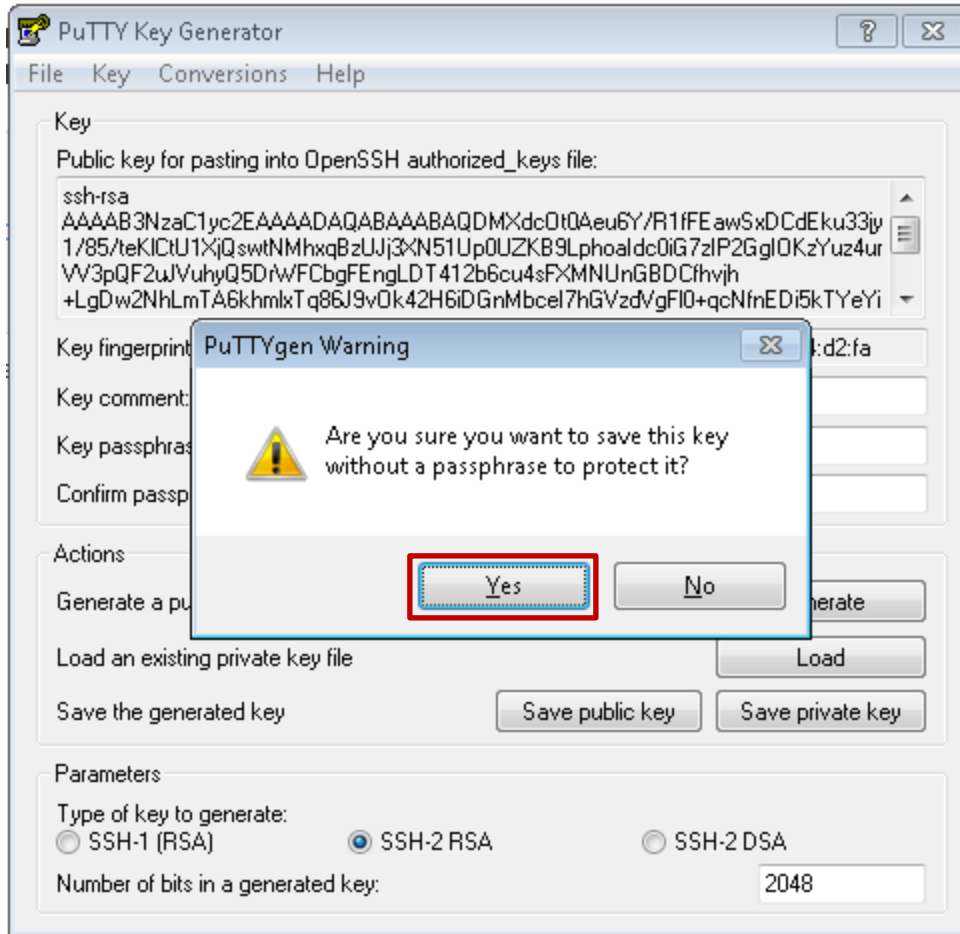
Note: Your host's downloads folder will contain different items then what is shown in the screenshot shown above.



5. You should receive a PuTTYgen Notice that the foreign key was successfully imported.
Click OK

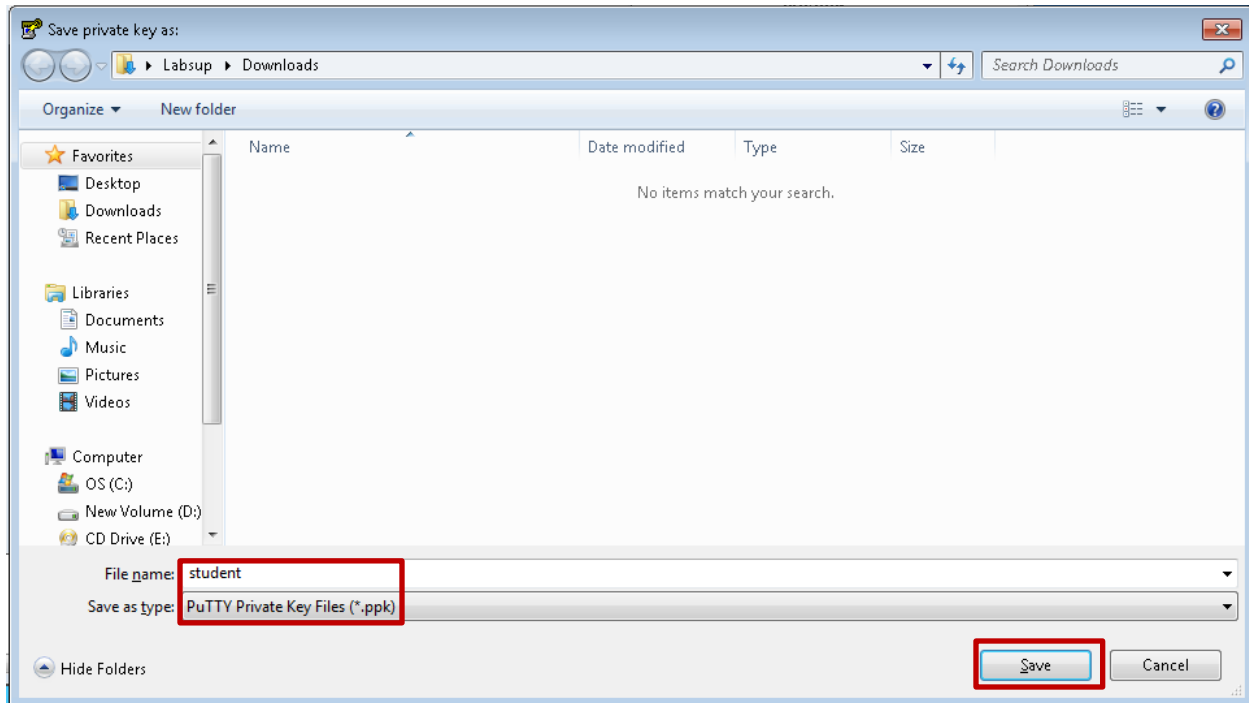


6. Click Save private key



7. Click Yes to save the key without a passphrase to protect it

Note: You may elect to create a passphrase to for additional security of your key pair outside of the training environment.



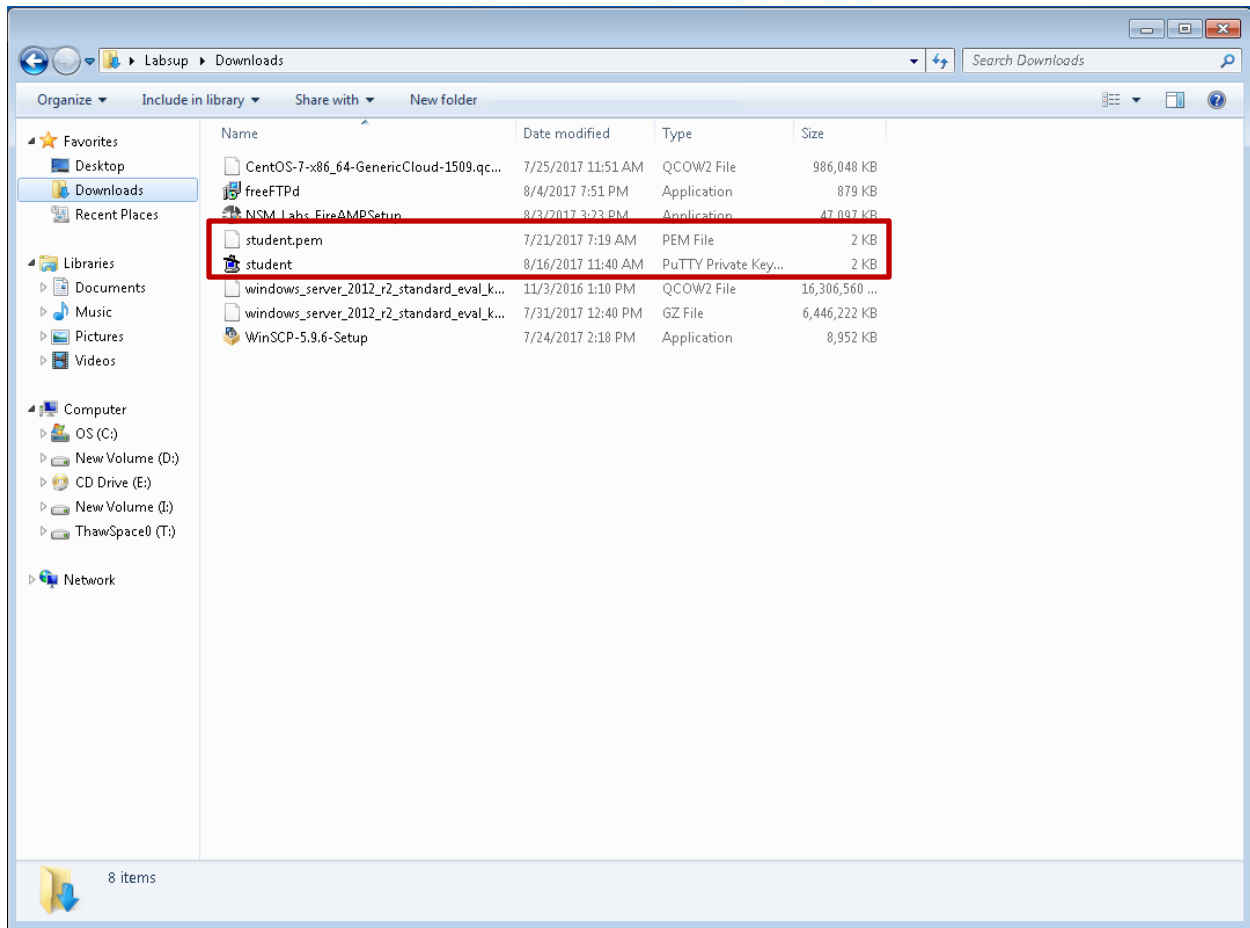
8. Enter the File name **student** and leave the default, Save as Type **PuTTY Private Key Files (*.ppk)** and **Click Save**.

Note: You can use the same file name, student, because the file extension is different .pem vs .ppk



9. **Close PuTTY Key Generator and open the Downloads folder**

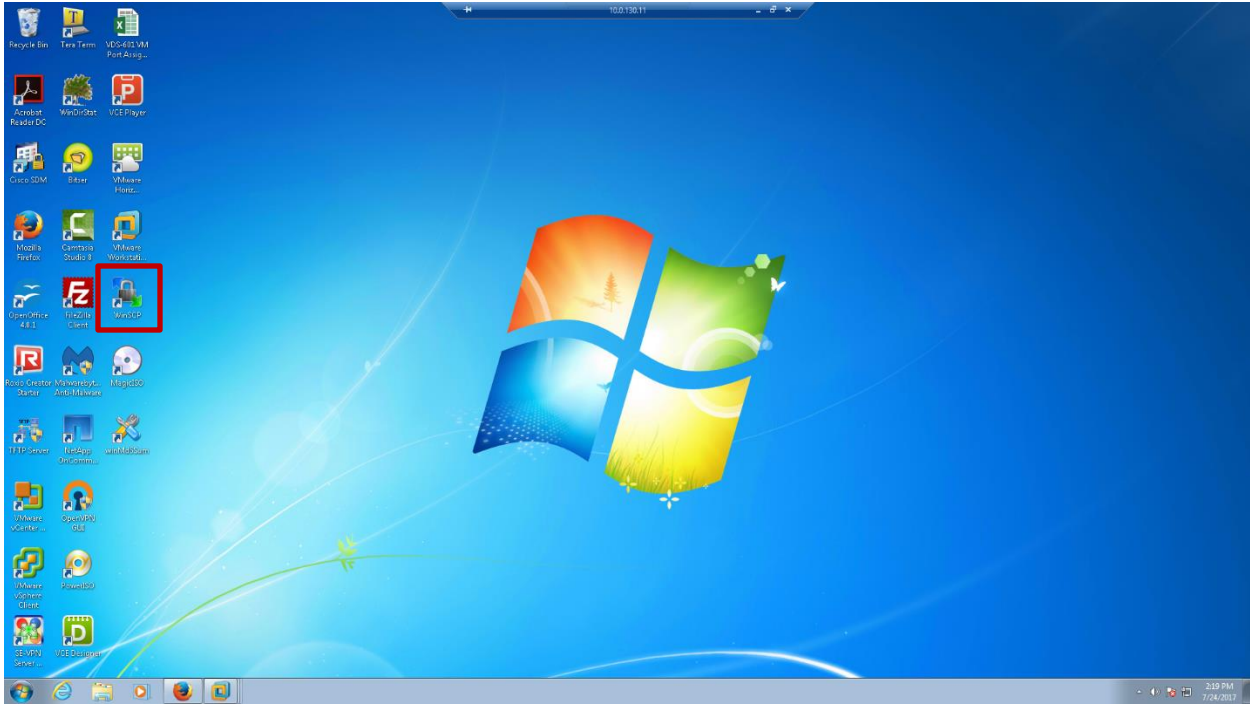
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



10. You should see that there are two student files, student.pem and student.ppk

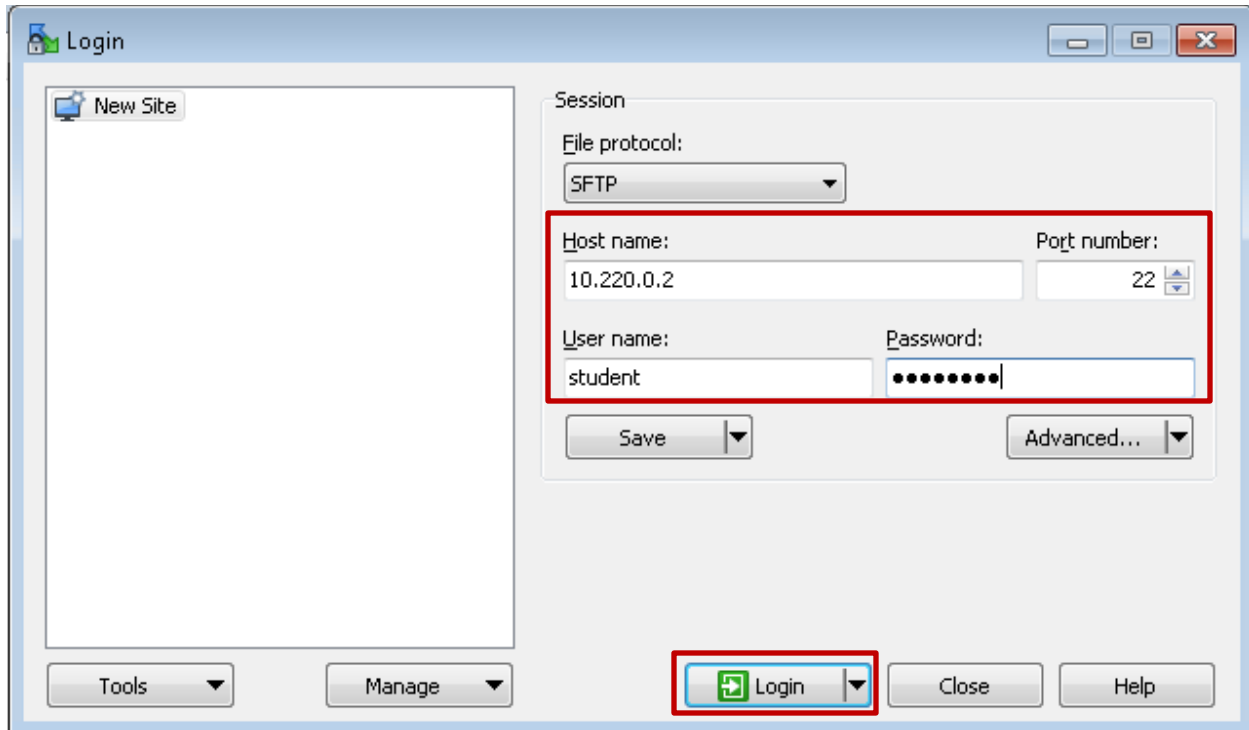
Note: Key Pairs are private and should be kept in a secure location and not shared with others. Normally they would kept in a file on the user's preferred OS or on a thumb drive in some cases.

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



11. Use WinSCP to copy the student.pem file to the Client2 VM (Linux OS) in the VMware Workstation environment, which you will later use to SSH to the instance from Client2's command line. **Double Click** on **WinSCP**.

Note: Your host may not have the WinSCP on the desktop.

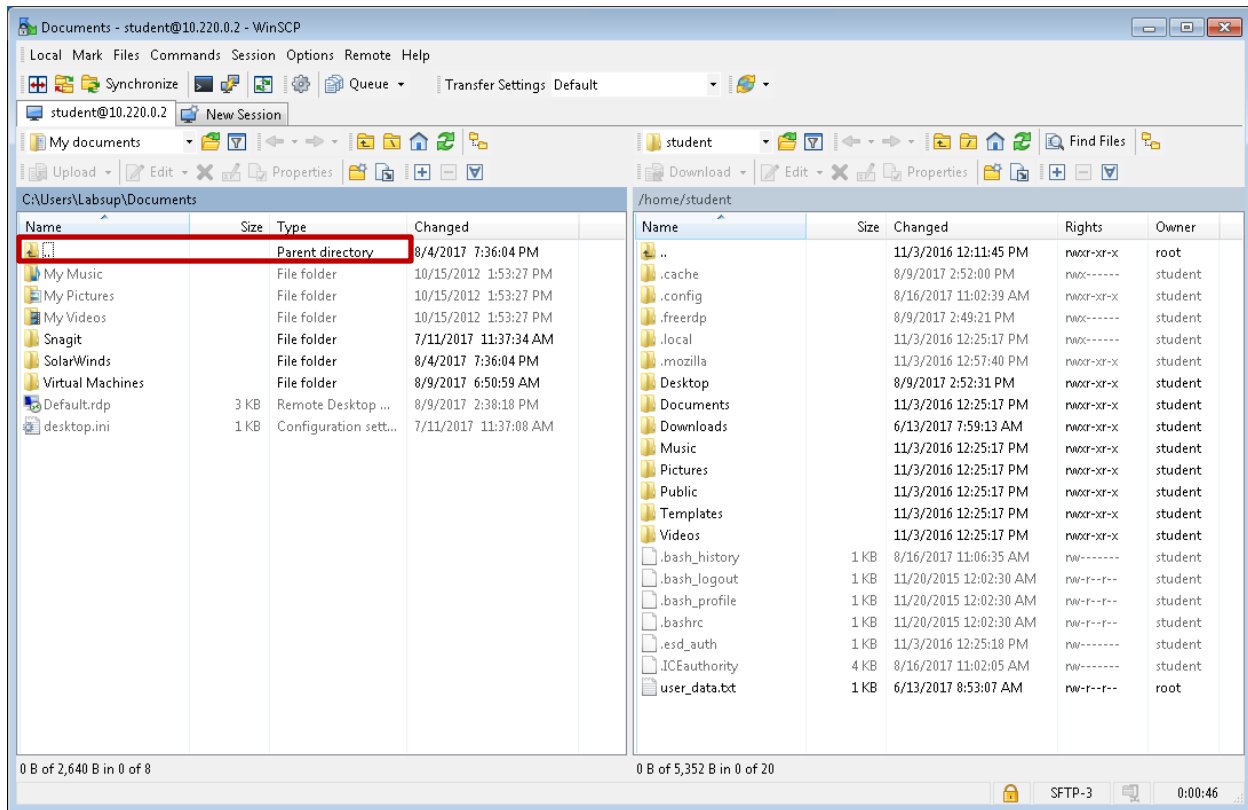


12. **Enter Client2's IP Address, username and password** in the lab settings section on page 6, and as shown in the screen capture above. **Click Login**

File protocol	SFTP (default)
Host name	10.220.0.2
Port number	22 (default)
User name	student
Password	P@ssword

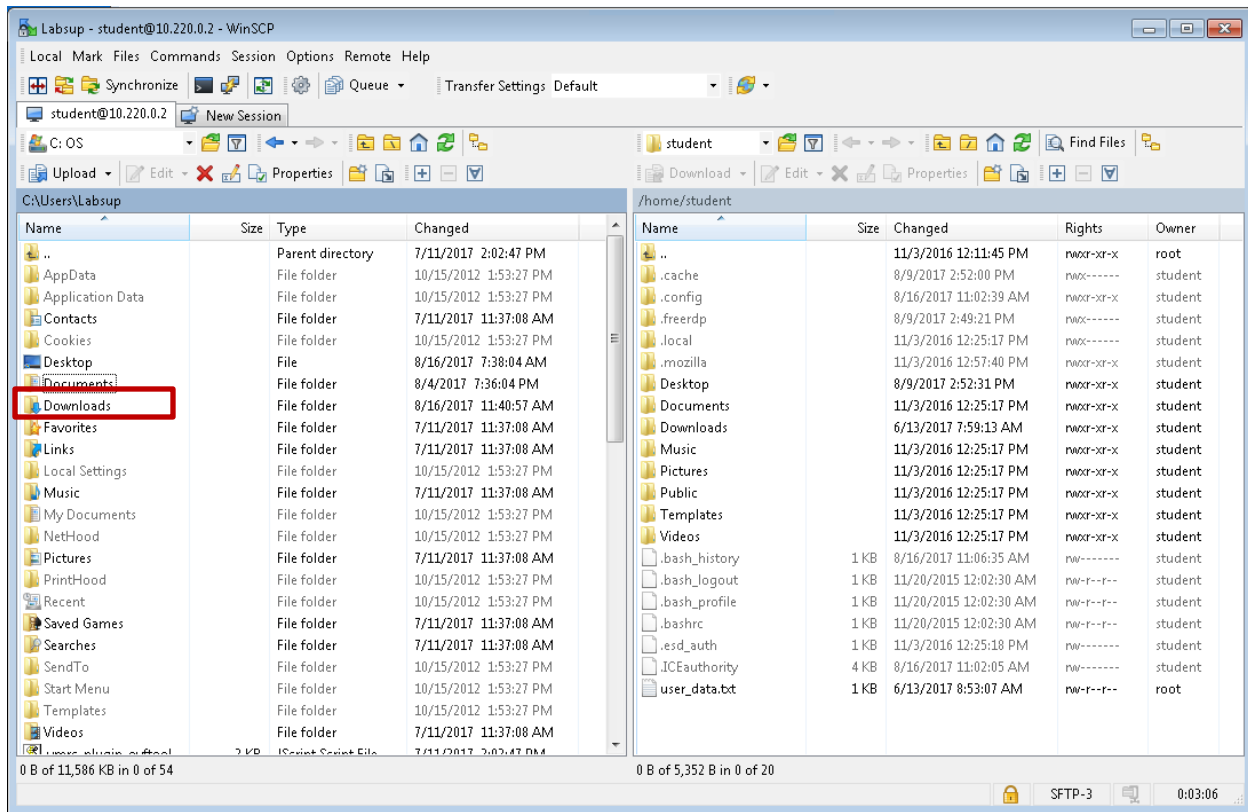


Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



- Once the connection is open, you should see that there are split folders. The left pane is the Windows host PC's C:\Users\Student1\Documents directory that you are in and in the right pane is the Openstack_WS_client2's /home/student directory. Starting in the left pane navigate to the Downloads folder by **double clicking** on the **folder icon** in the parent directory row

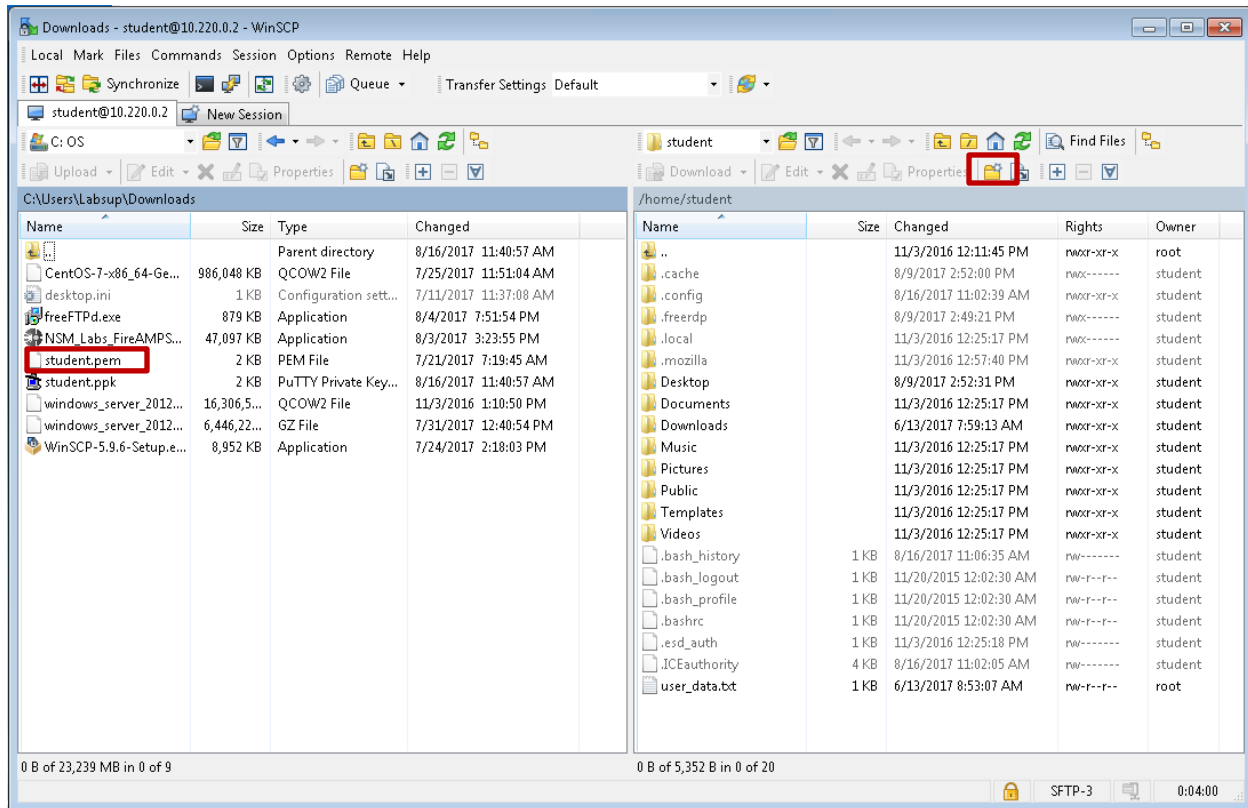
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



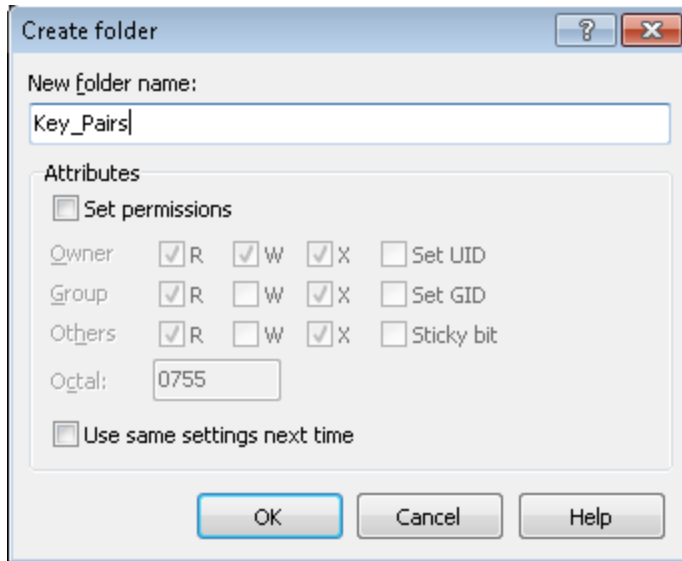
14. Double Click on the **Downloads** folder in the left pane



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair

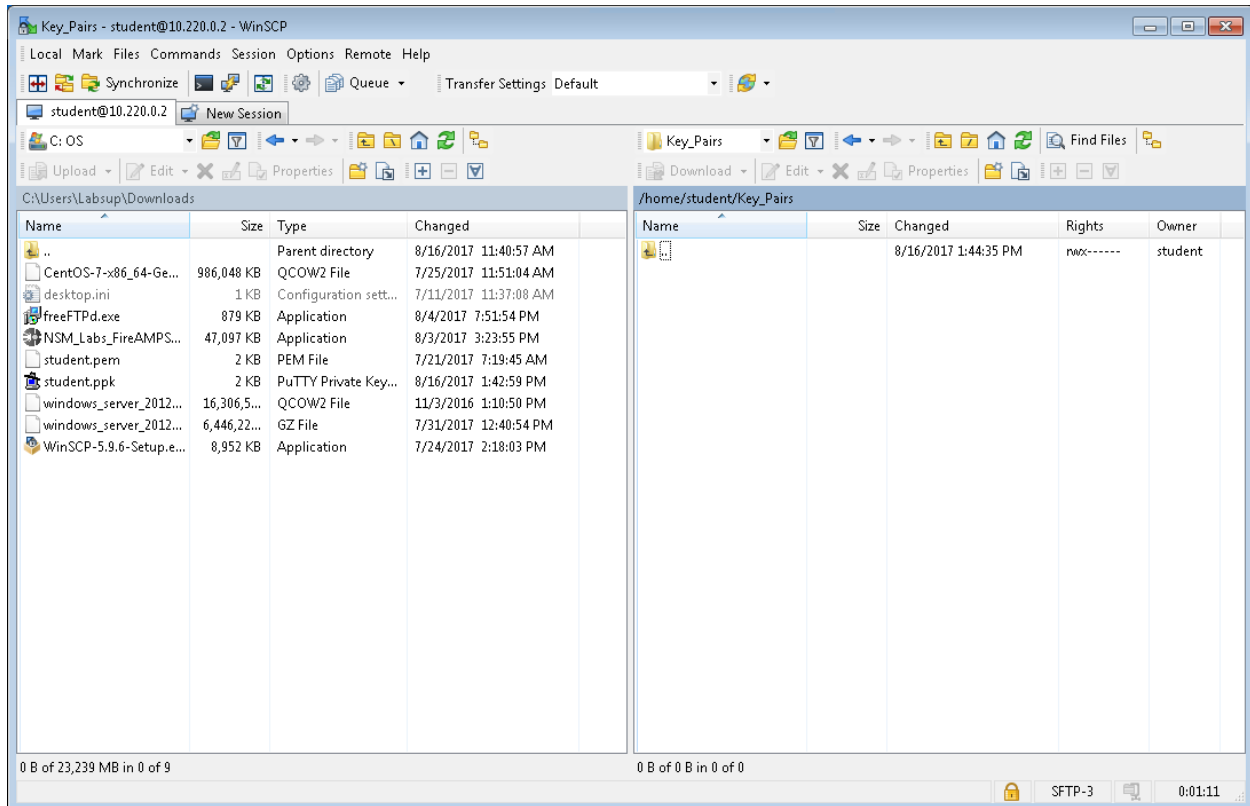


15. Check for the **student.pem** file, then **Double Click** to open the **Create directory** folder above the right pane.



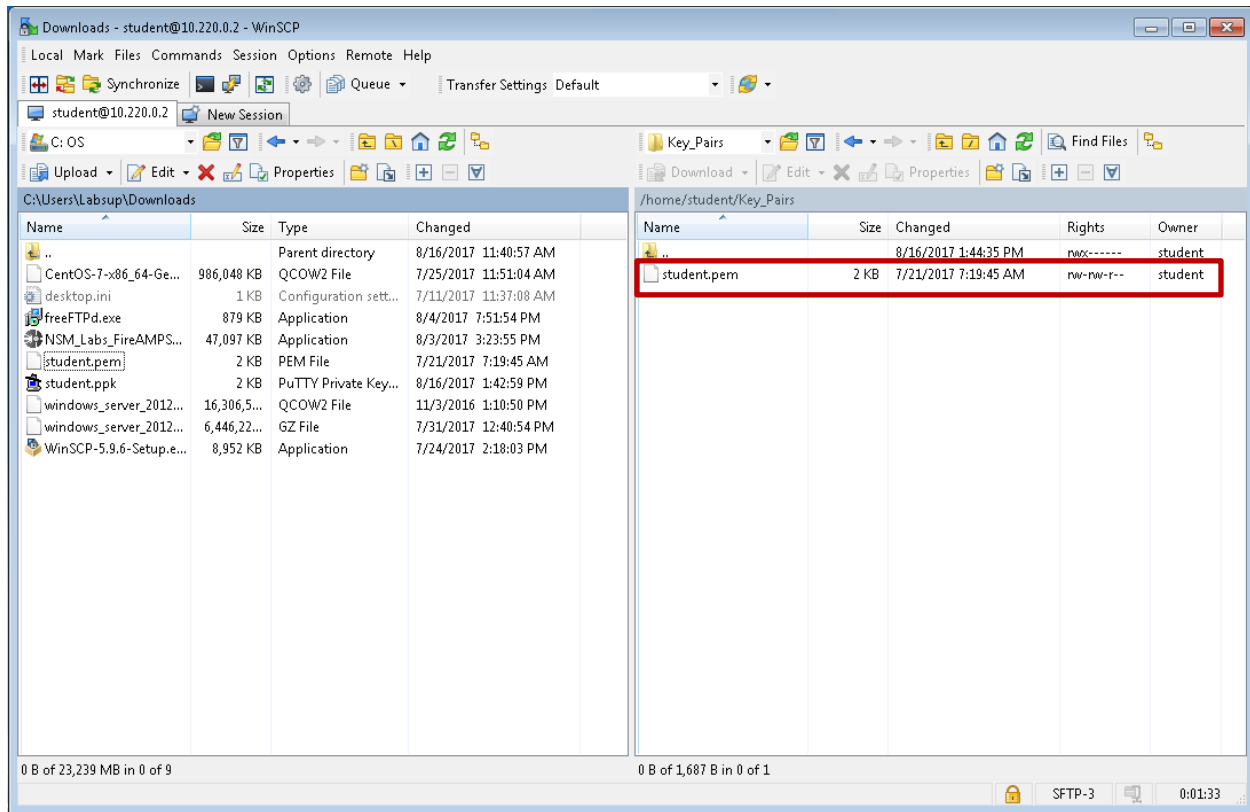
16. **Name** the new folder **Key_Pairs** and **double click** to open the **new Key Pairs folder** (shown on next page).

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



17. Click and hold on the **student.pem** file in the left pane and drag it to right pane.

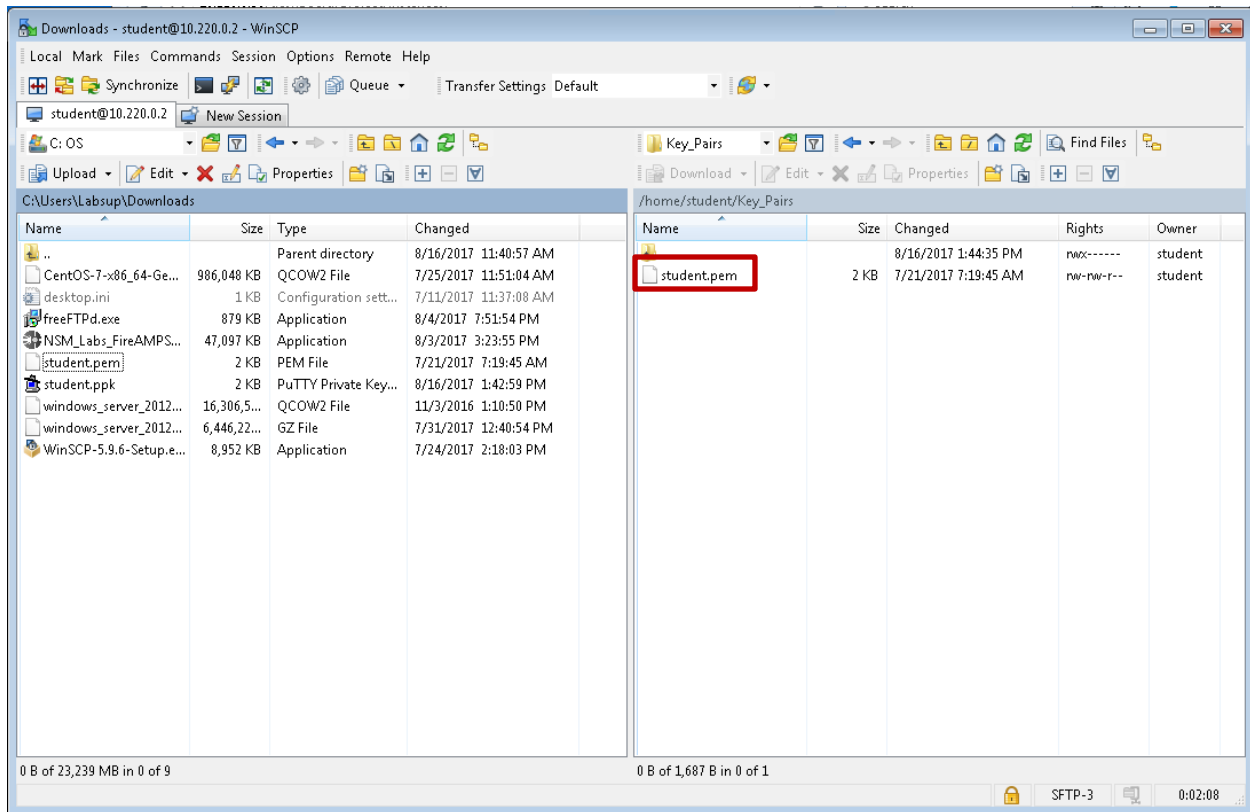
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



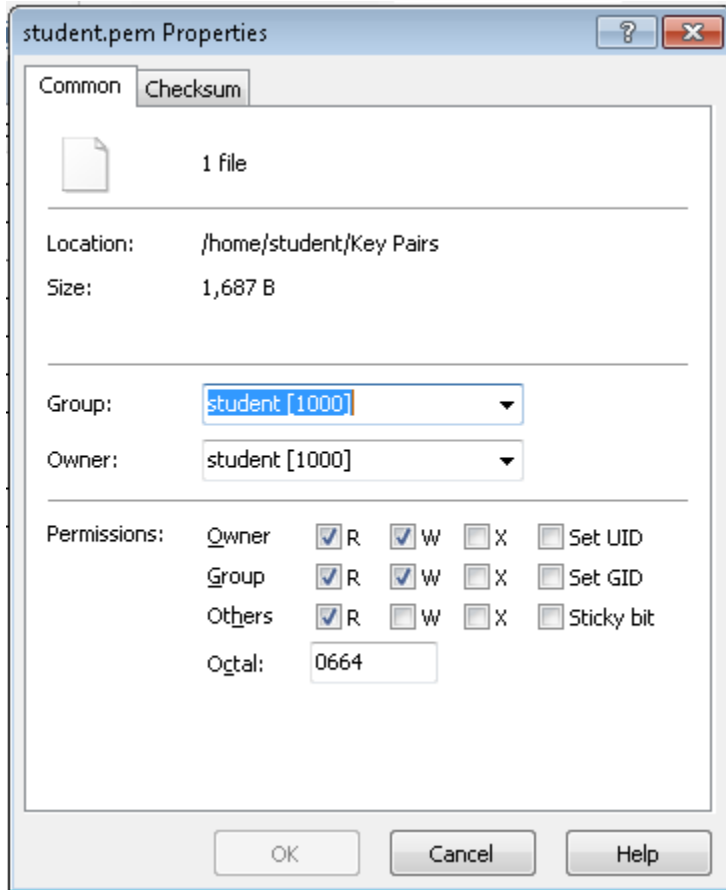
18. Verify that the **student.pem** file has been copied to the **Client2 VM**.

Note: The file rights are rw-rw-r--

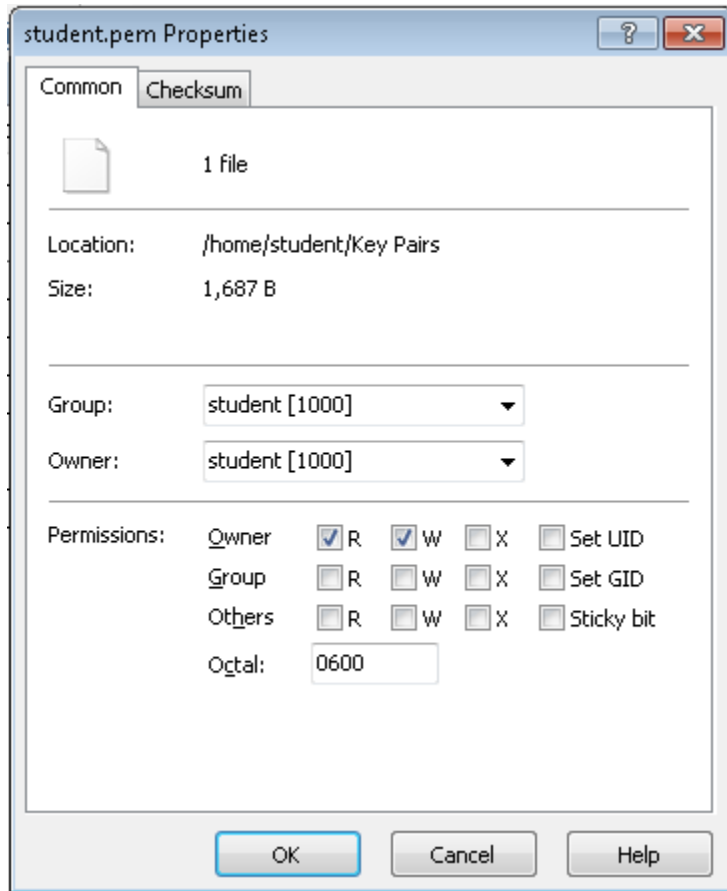
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



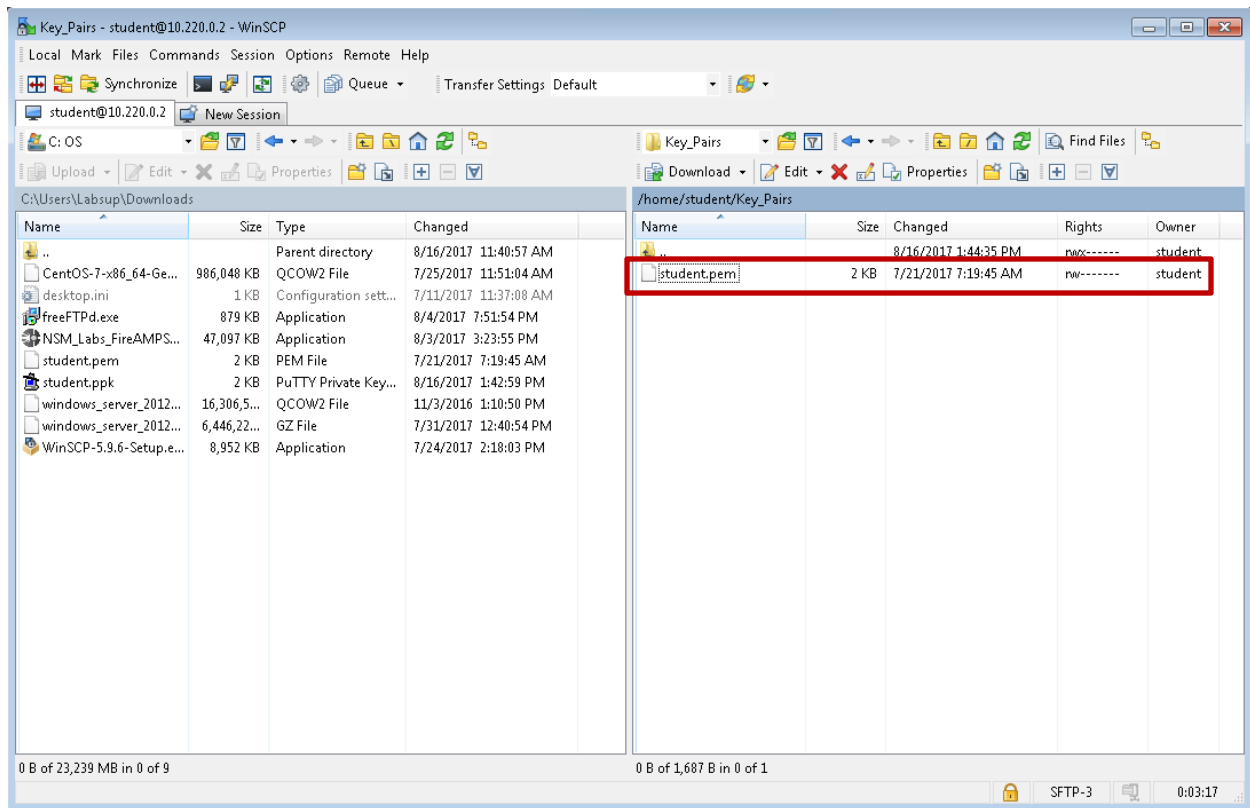
19. To use the student.pem file (or any *.pem file) to SSH into another machine from a Linux OS, you must first change the properties of the file. In the right pane, **right click** on the **student.pem** file and **select Properties**



20. **Deselect the Group Read/Write and Others Read permissions** on the student.pem file.
Shown on next page



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



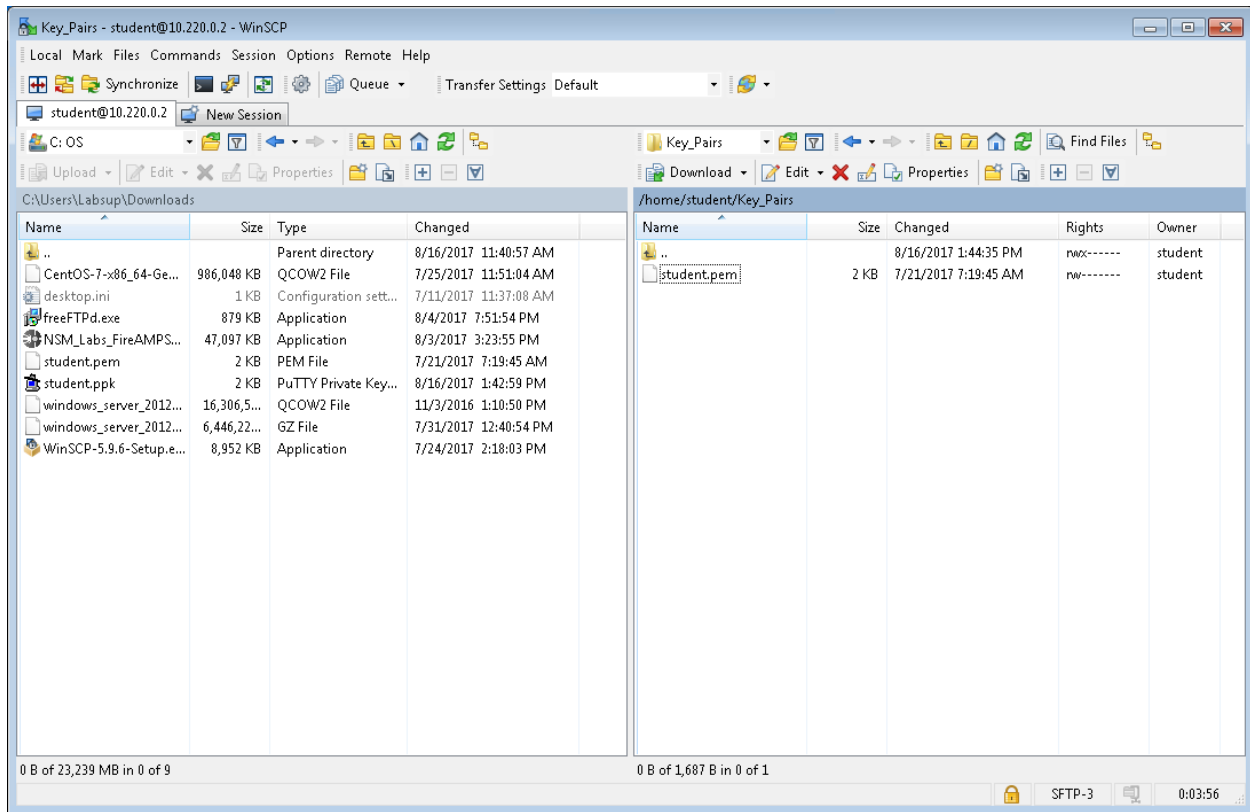
21. **After** Deselecting the Group and Other permissions on the student.pem file, as shown in the screen capture above. **Click OK**

Note: The file rights are now rw-----

Key Pairs

Changing the permissions can also be completed from the Linux terminal using the `chmod 600 key_name.pem` command.

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair

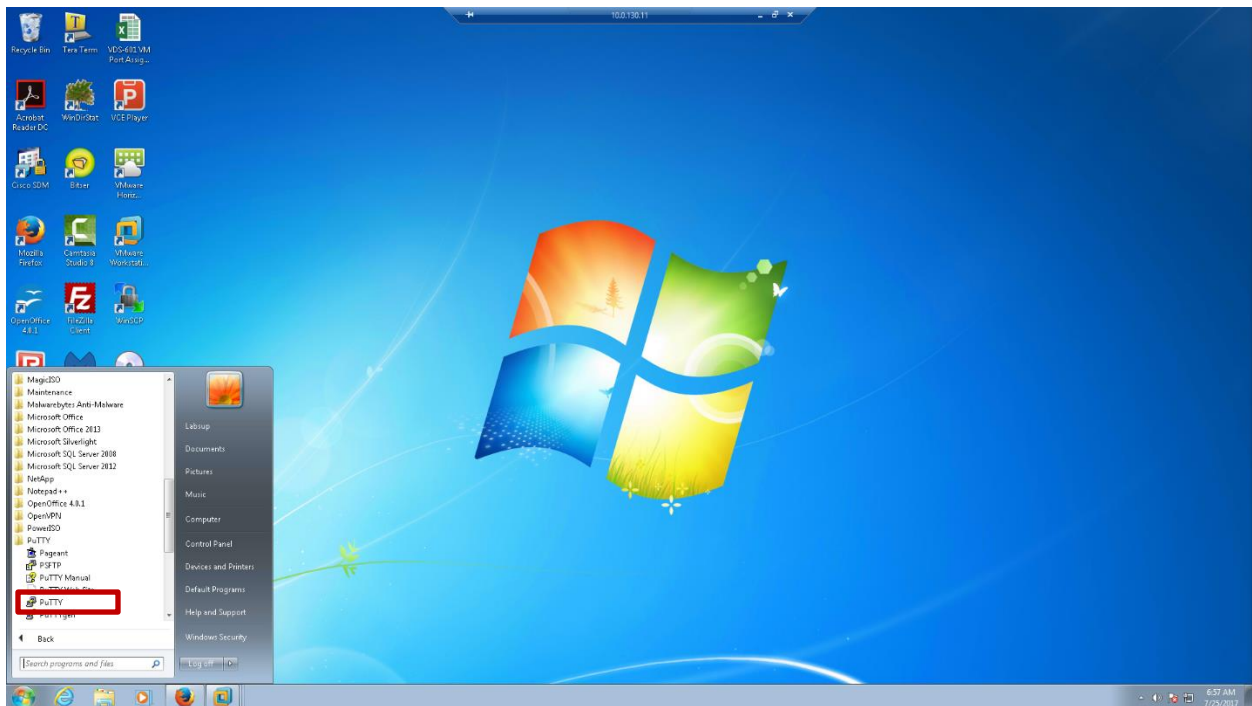


22. The student.pem and student.ppk files are ready for use. Next you will connect to an instance using PuTTY on a Windows host and SSH from the command line on a Linux VM. **Close WinSCP.**

Continue to Lab 15.



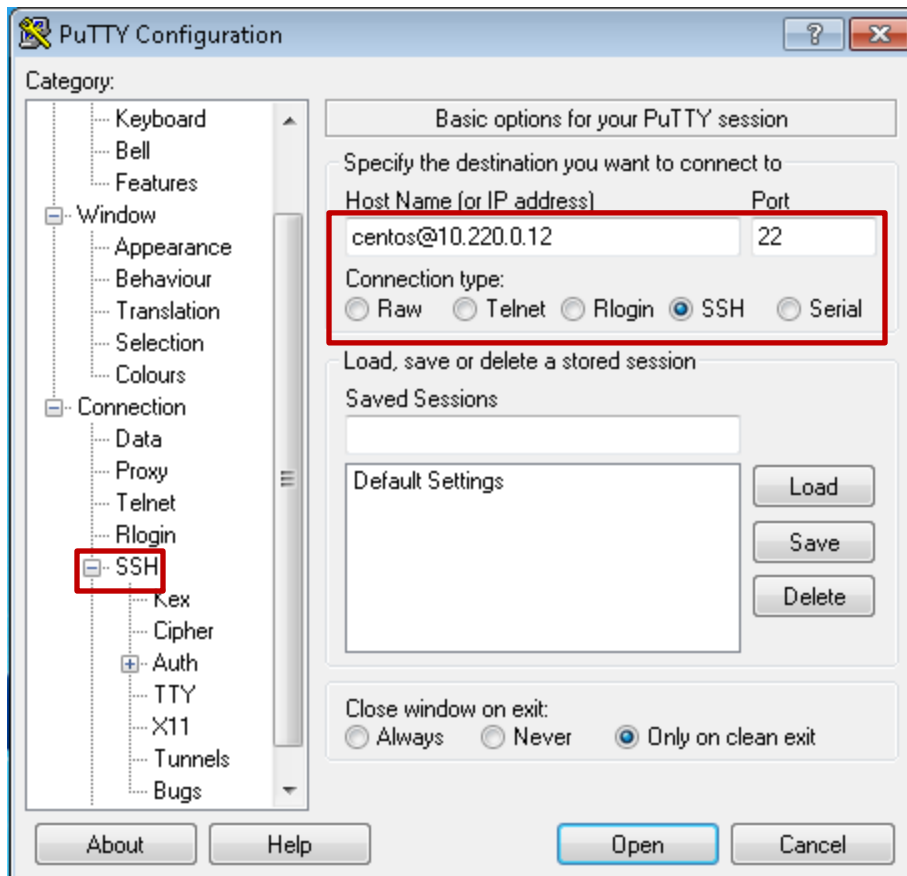
Lab 15: Connect to an Instance using PuTTY on Windows



1. Open the console to Client1 and **double click** on the **PuTTY** icon on the desktop

Security Groups

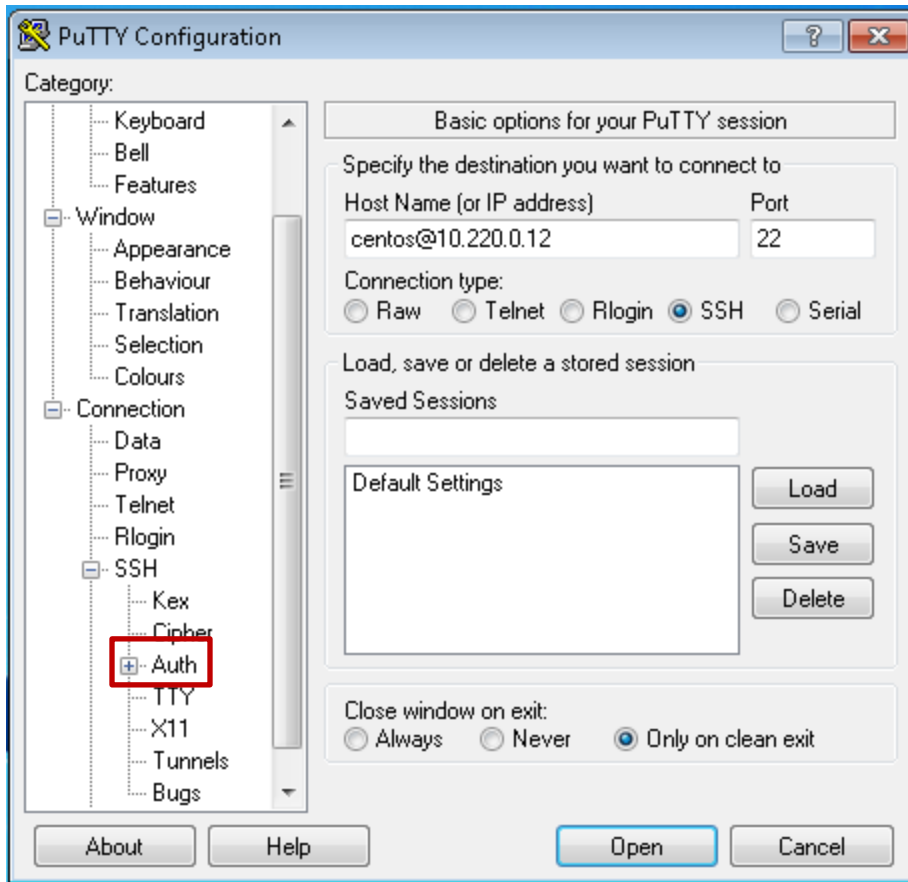
Remember, by default all inbound network traffic is blocked for both IPv4 and IPv6. You must add a rule to open any port or protocol that you want available to an instance. For example: SSH, HTTP, HTTPS, ICMP, port number (1-65535), or even a custom rule.



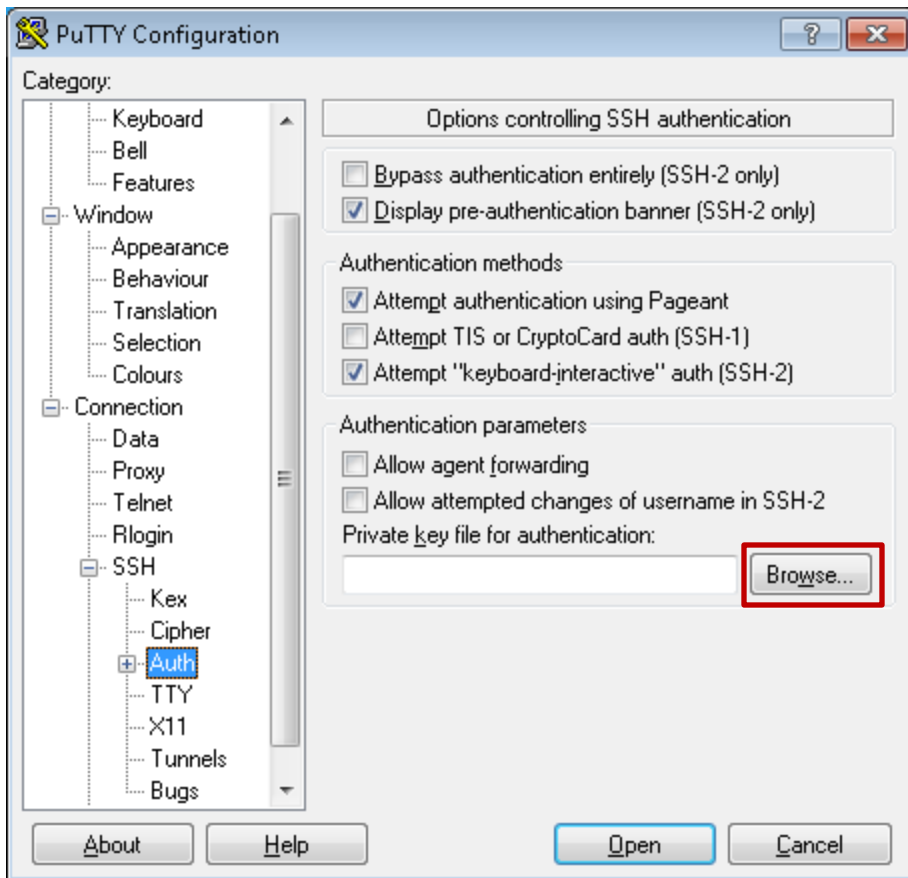
2. Enter the **username centos** and **public IP address** of the Instance that you are connecting to in the following format **centos@10.220.0.12** and **Click** on the + adjacent to **SSH** in the left pane. Leave **Port 22** and **Connection type SSH** at the default settings.

Note: You can view the OpenStack instance IP address information from the OpenStack dashboard

Note: Instances can use different usernames for example; centos, cloud-user, administrator and others, so be sure to check what username is valid for the image that you are using to build an instance. The usernames are often referred to as “baked in usernames”

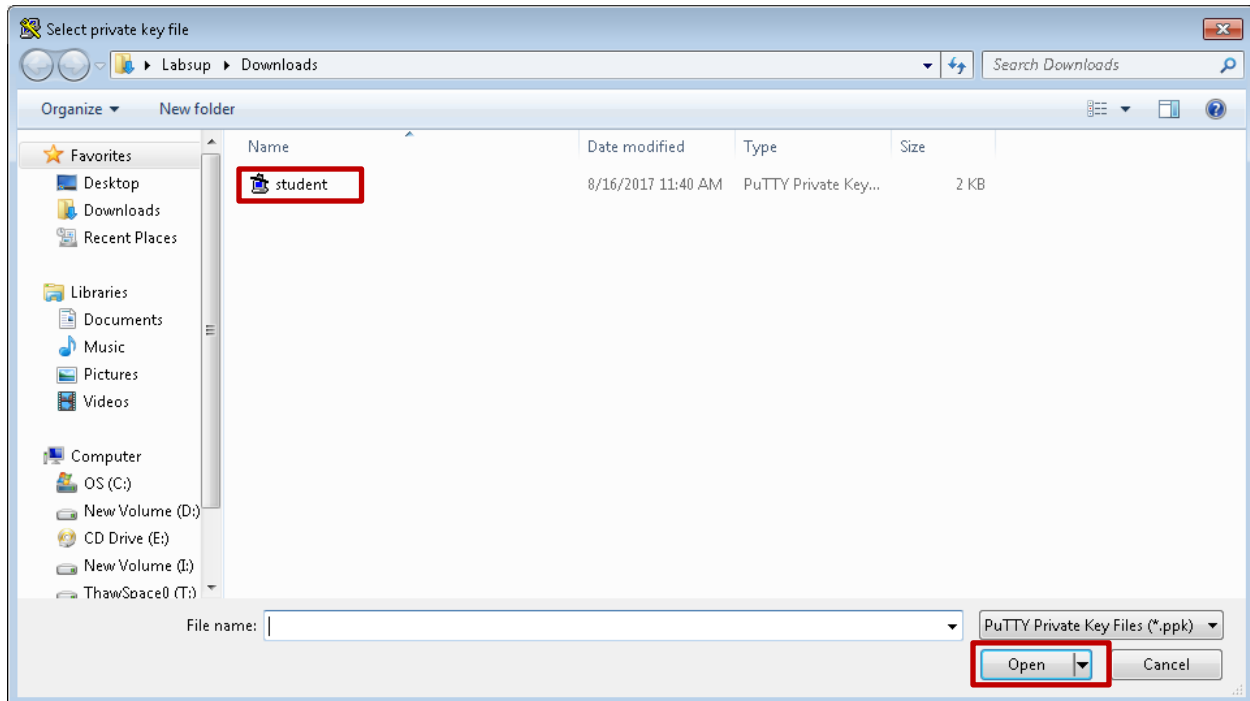


3. **Click on Auth**

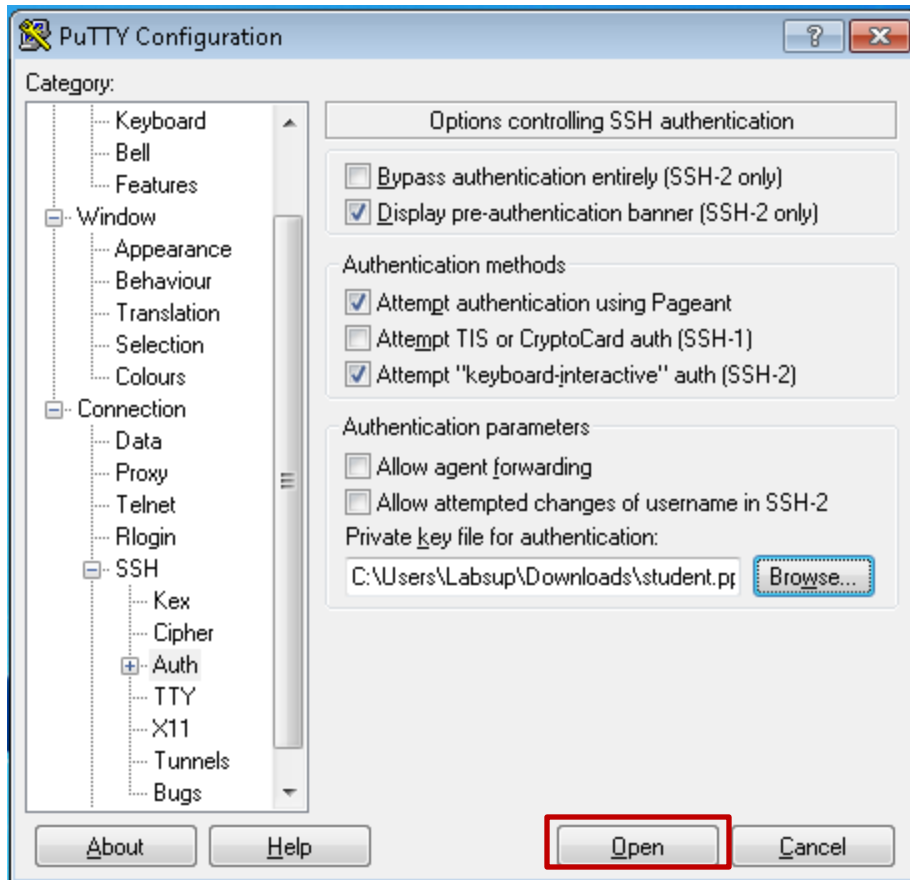


3. Click on Browse

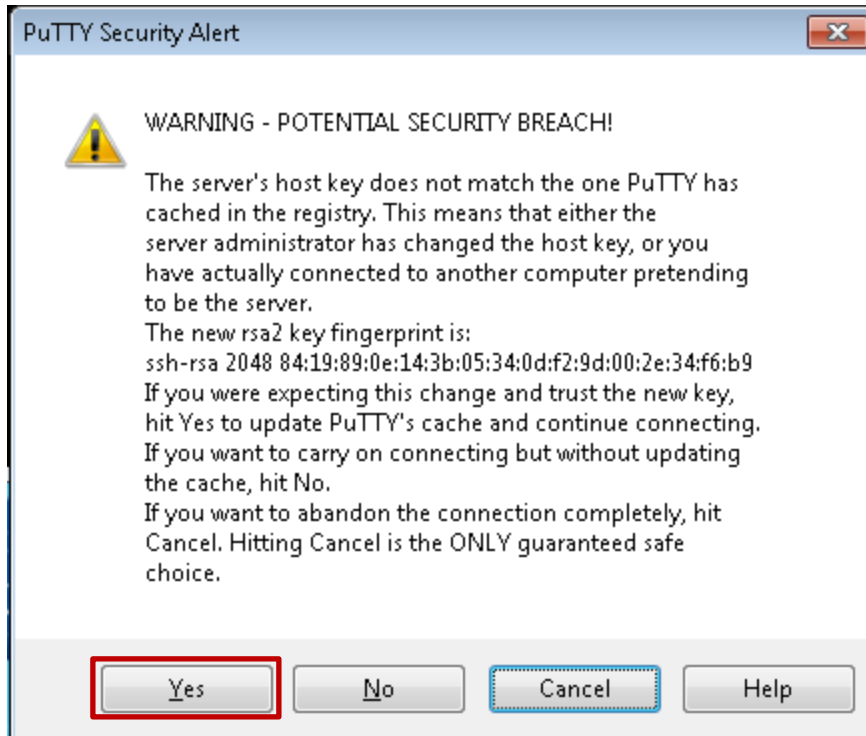
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



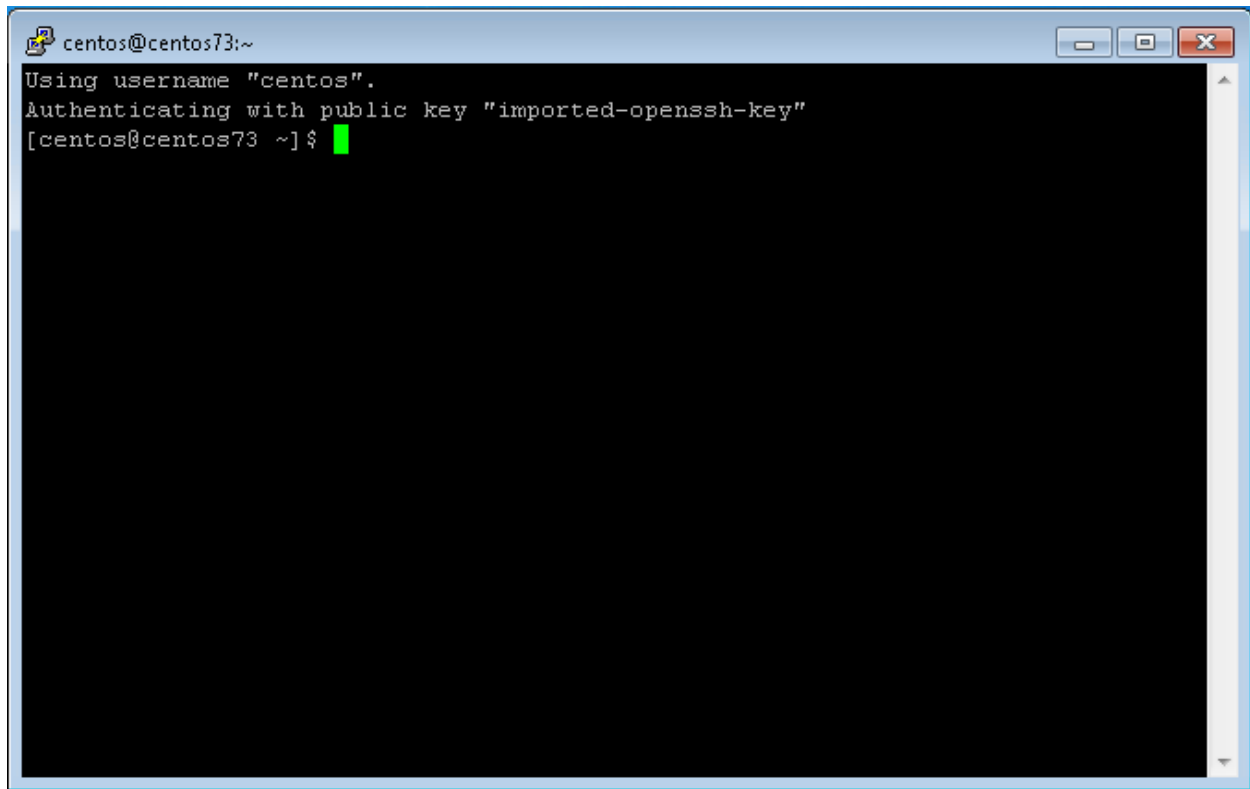
4. Select the **student.ppk** and click **Open**



5. Click Open



6. If you see this PuTTY Security Alert, **Click on Yes**

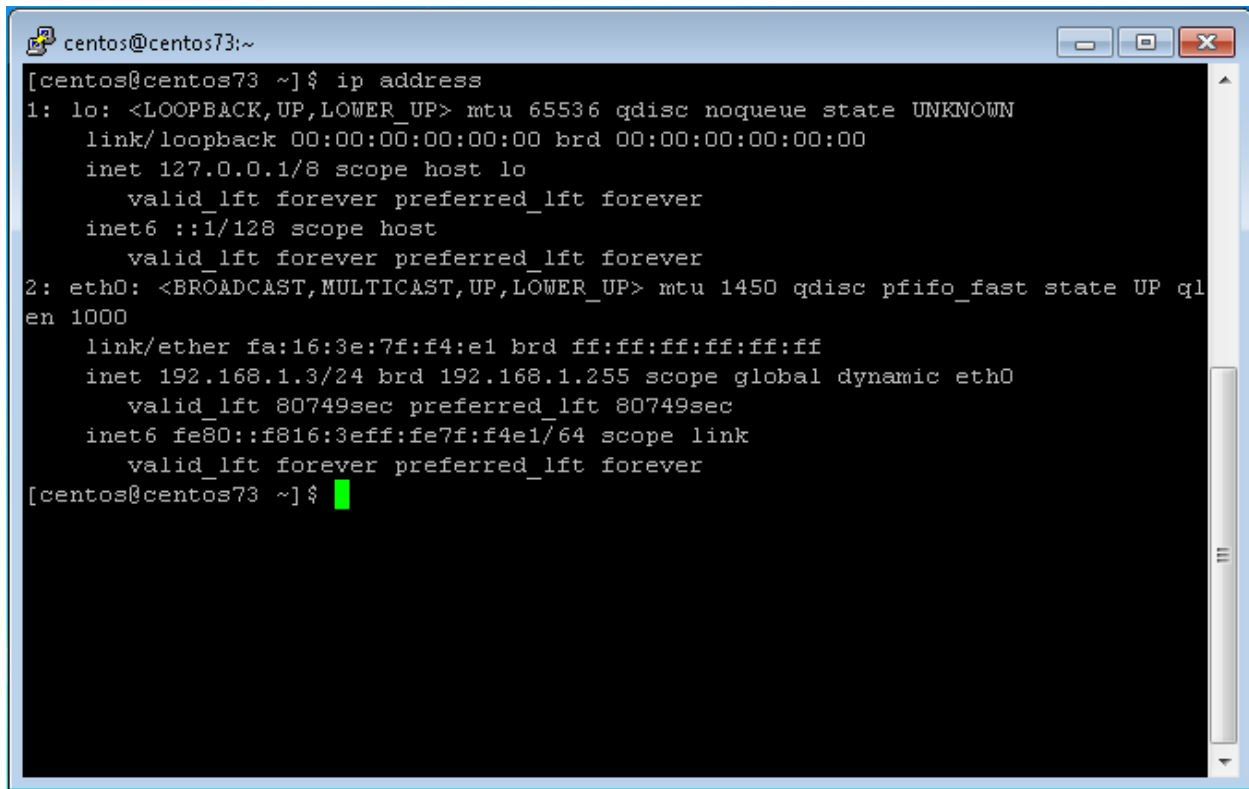
A terminal window with a blue title bar. The title bar contains a small icon on the left and three window control buttons (minimize, maximize, close) on the right. The text inside the terminal is as follows:

```
centos@centos73:~  
Using username "centos".  
Authenticating with public key "imported-openssh-key"  
[centos@centos73 ~]$
```

A green cursor is visible at the end of the last line.

7. You are now connected to the CentOS7 instance console via SSH using PuTTY installed on a Windows VM.

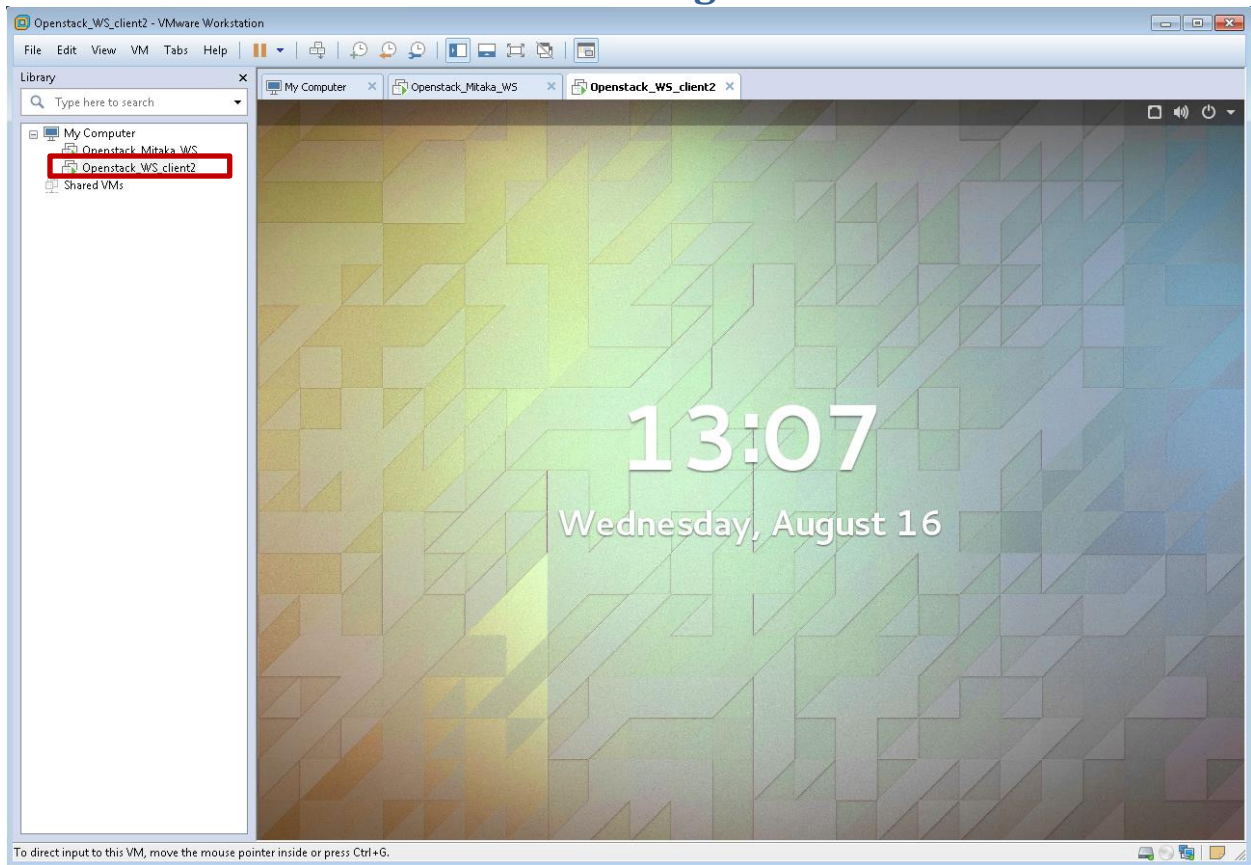
Note: The Instance name centos73 doesn't match the CentOS7#3 name you assigned. This is because the BASH shell treats the # symbol as a special character.



```
centos@centos73:~  
[centos@centos73 ~]$ ip address  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pfifo_fast state UP qlen 1000  
    link/ether fa:16:3e:7f:f4:e1 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic eth0  
        valid_lft 80749sec preferred_lft 80749sec  
    inet6 fe80::f816:3eff:fe7f:f4e1/64 scope link  
        valid_lft forever preferred_lft forever  
[centos@centos73 ~]$
```

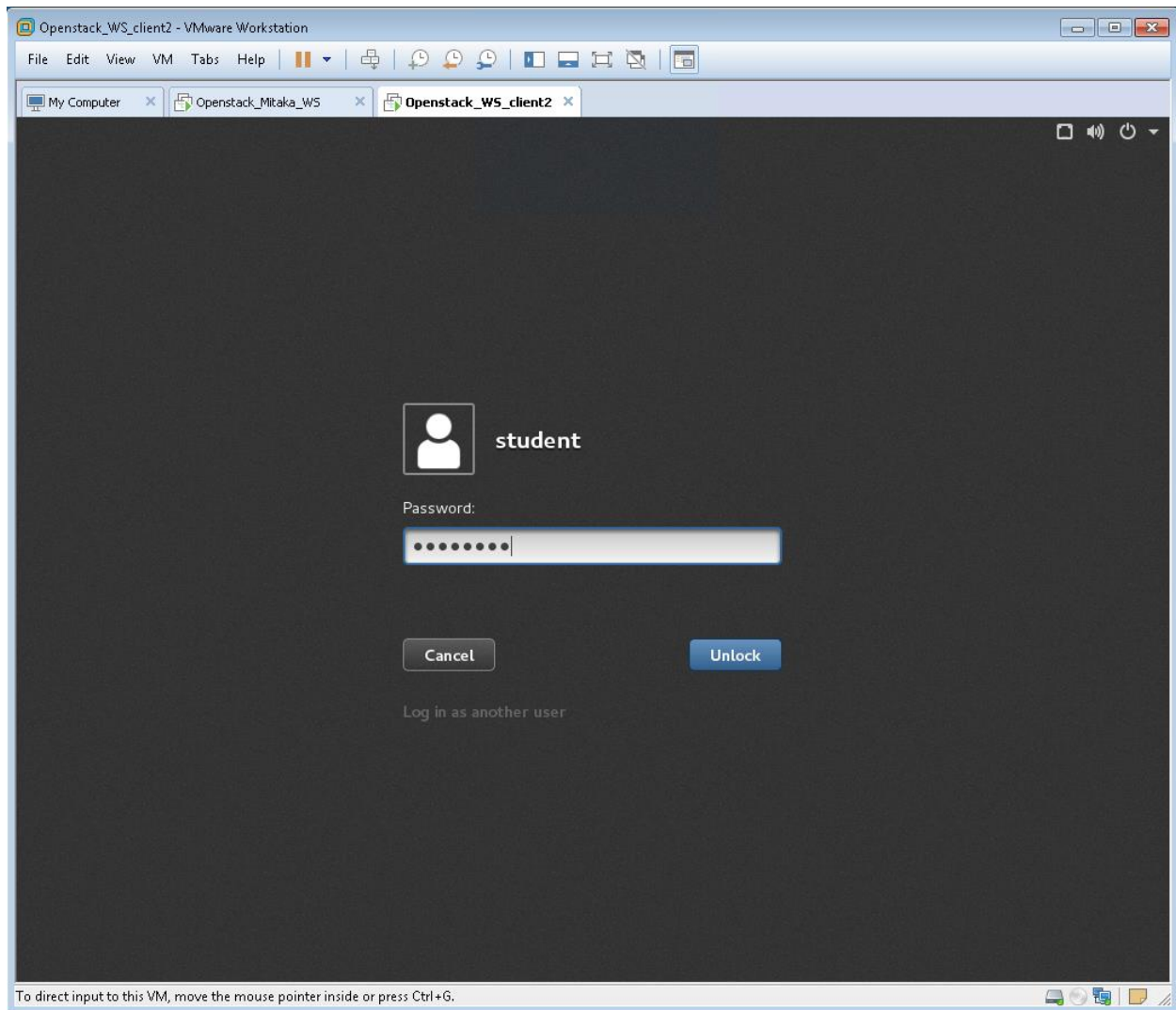
8. **Type `ip address` and press Enter.** You should see the private IP address of 192.168.1.3 was assigned by DHCP by the OpenStack neutron service when the instance was launched. We used the IP address 10.220.0.12 in PuTTY to connect from the Windows VM, why don't we see the IP address 10.220.0.12 now? Close the SSH session to CentOS7#3 and return to VMware Workstation NETLAB for Lab 6.3

Lab 16: Connect to an Instance using the command line in Linux



1. Click on **Openstack_WS_client2**

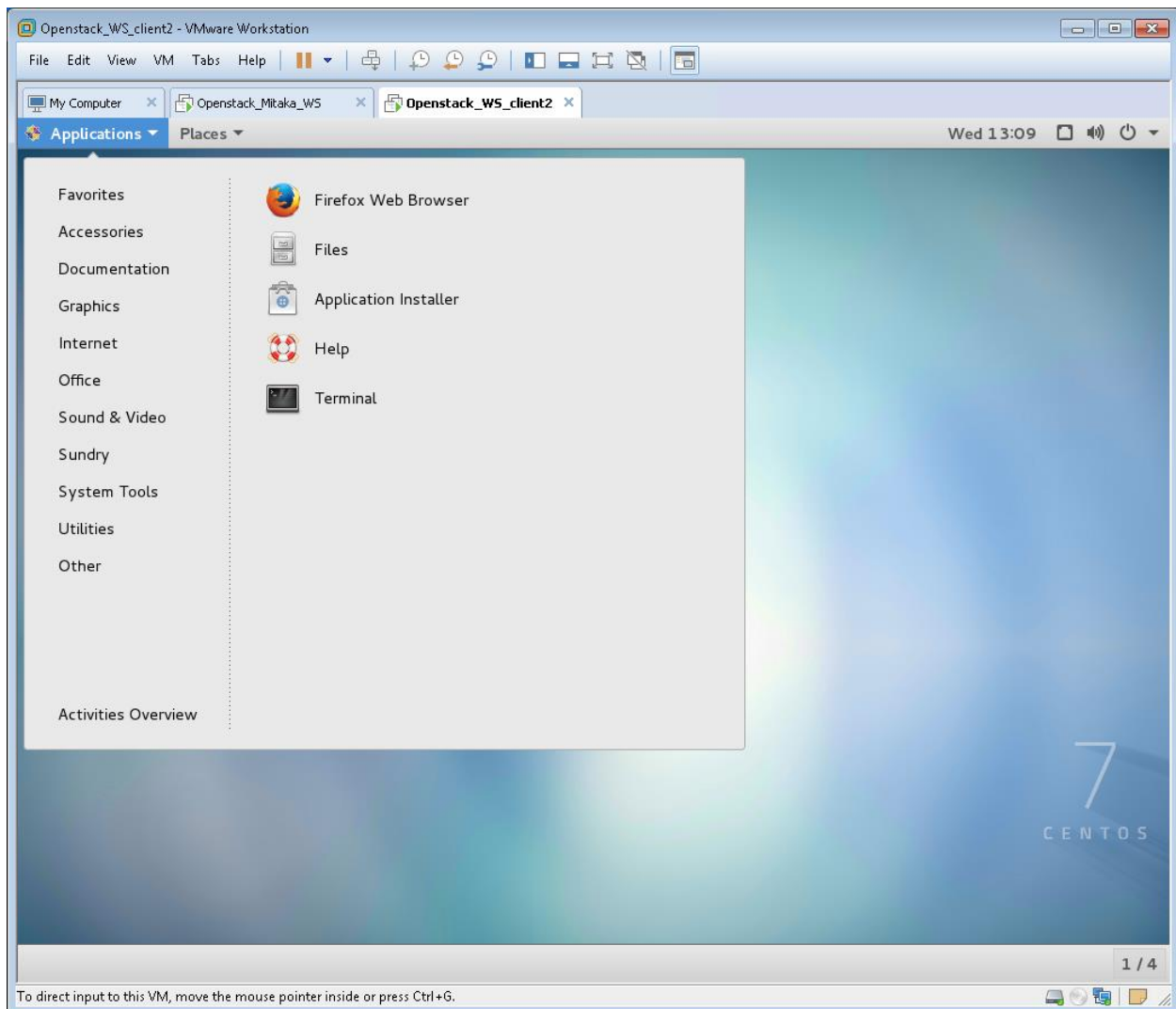
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



2. Login as **student** with **P@ssword**

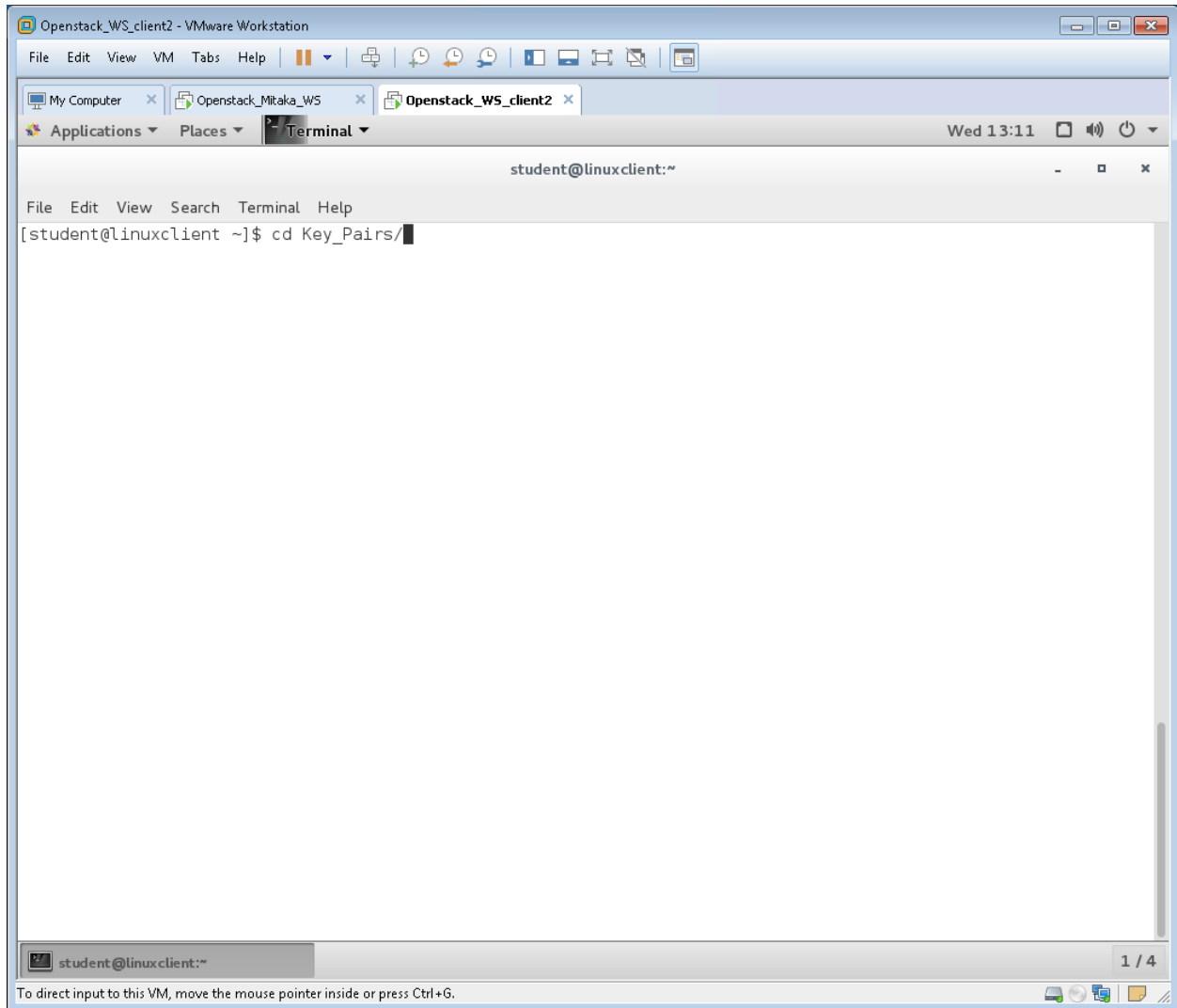
Note: If the CentOS VM screen doesn't show the login prompt, tap the spacebar

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



3. From the Applications dropdown menu, **select Favorites** and **Click on Terminal**

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair

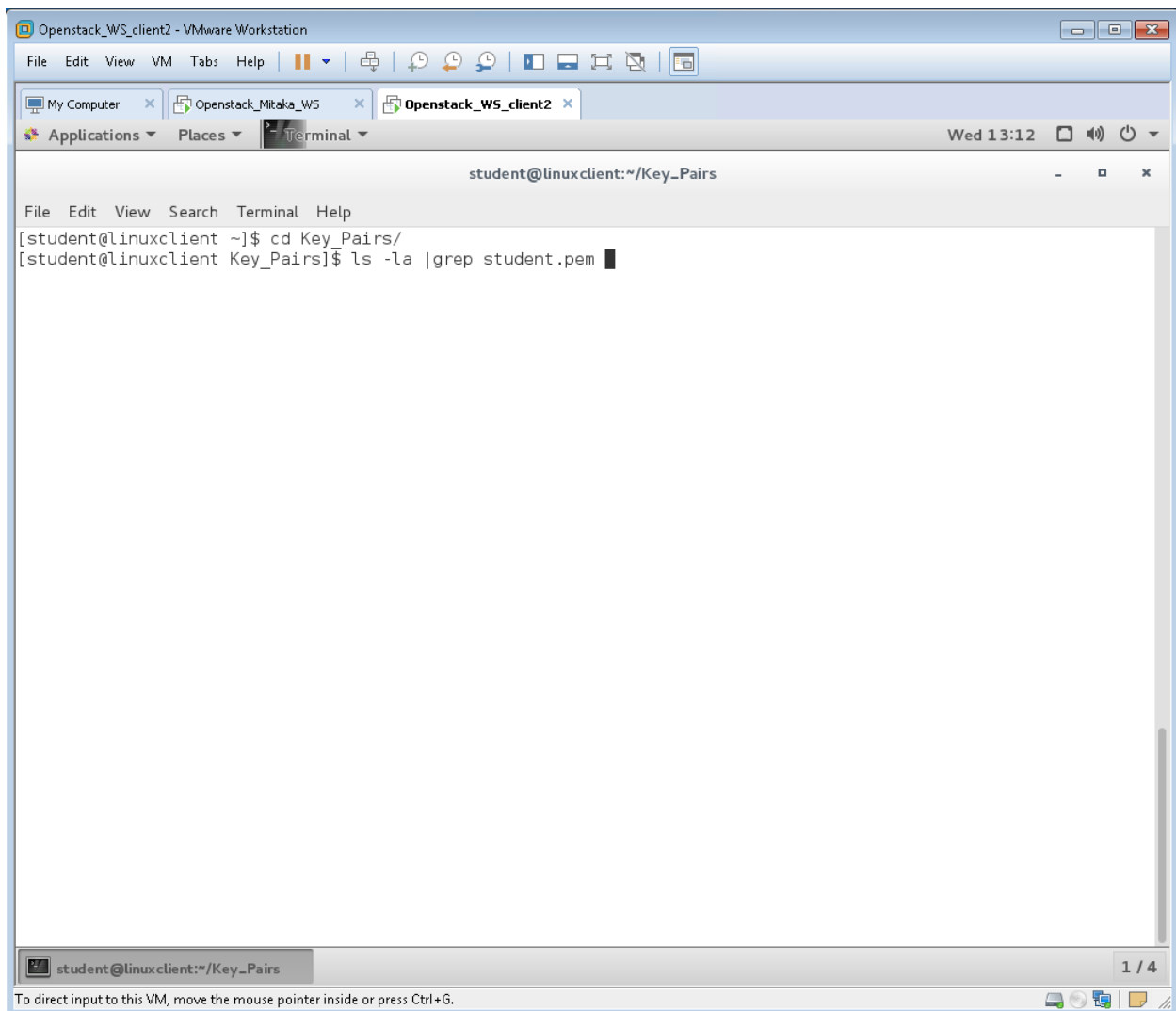


4. After the terminal is open; you will check that the student.pem key pair is present. **Type cd Key_Pairs and press Enter**

Note: cd is the change directory command



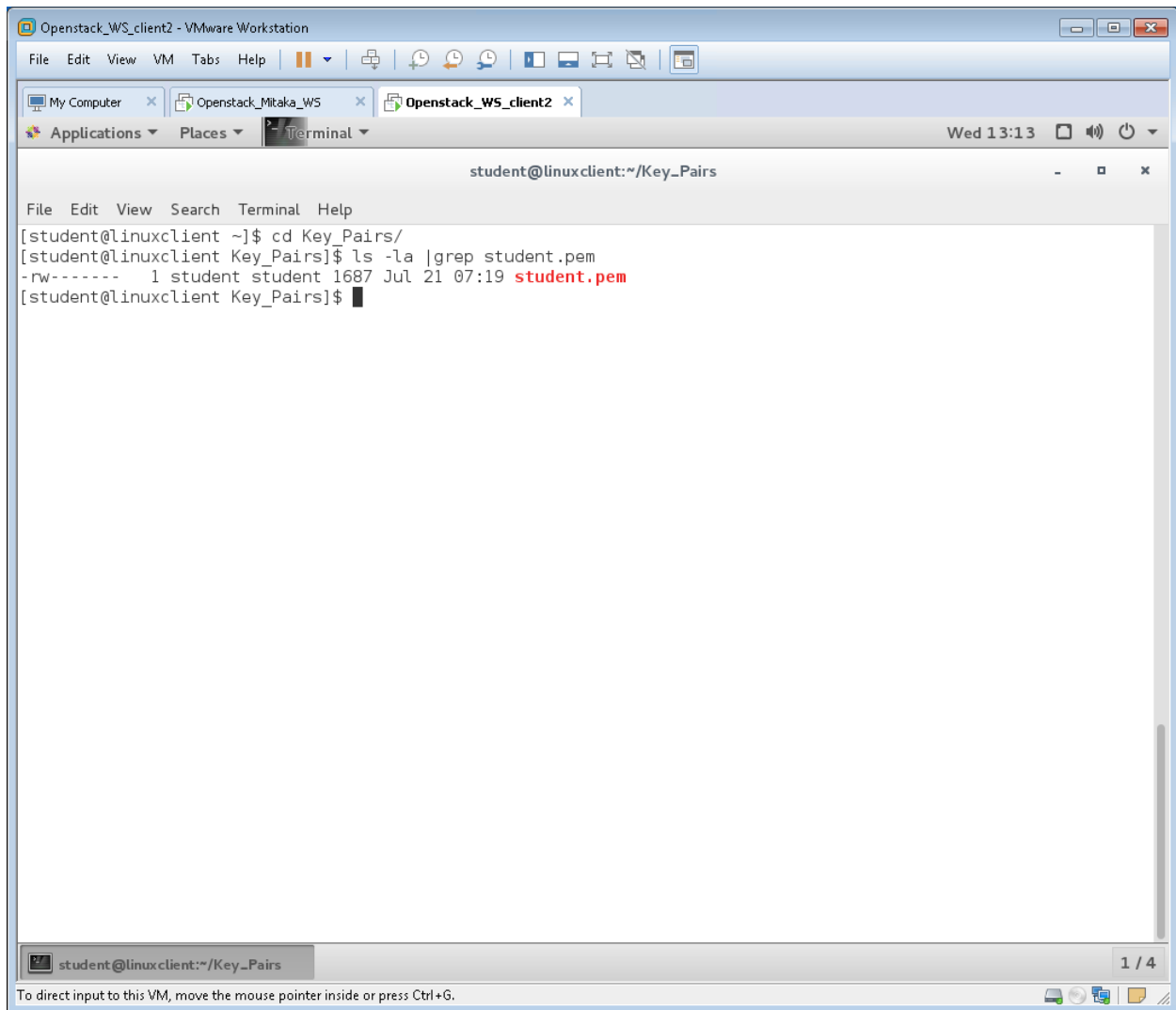
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



5. From the Downloads folder, **type `ls -l | grep student.pem`** and **press Enter**

Note: **`ls -l`** is the command to list the files, in long form (-l), in the working director, and the **|** (pipe) symbol is the command to direct the standard output of one command into the input of another command, and the **`grep`** command is used to search for a string of characters that matches the specific pattern.

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



```
Openstack_WS_client2 - VMware Workstation
File Edit View VM Tabs Help
My Computer Openstack_Mitaka_WS Openstack_WS_client2
Applications Places Terminal
Wed 13:13

student@linuxclient:~/Key_Pairs

File Edit View Search Terminal Help
[student@linuxclient ~]$ cd Key_Pairs/
[student@linuxclient Key_Pairs]$ ls -la |grep student.pem
-rw----- 1 student student 1687 Jul 21 07:19 student.pem
[student@linuxclient Key_Pairs]$
```

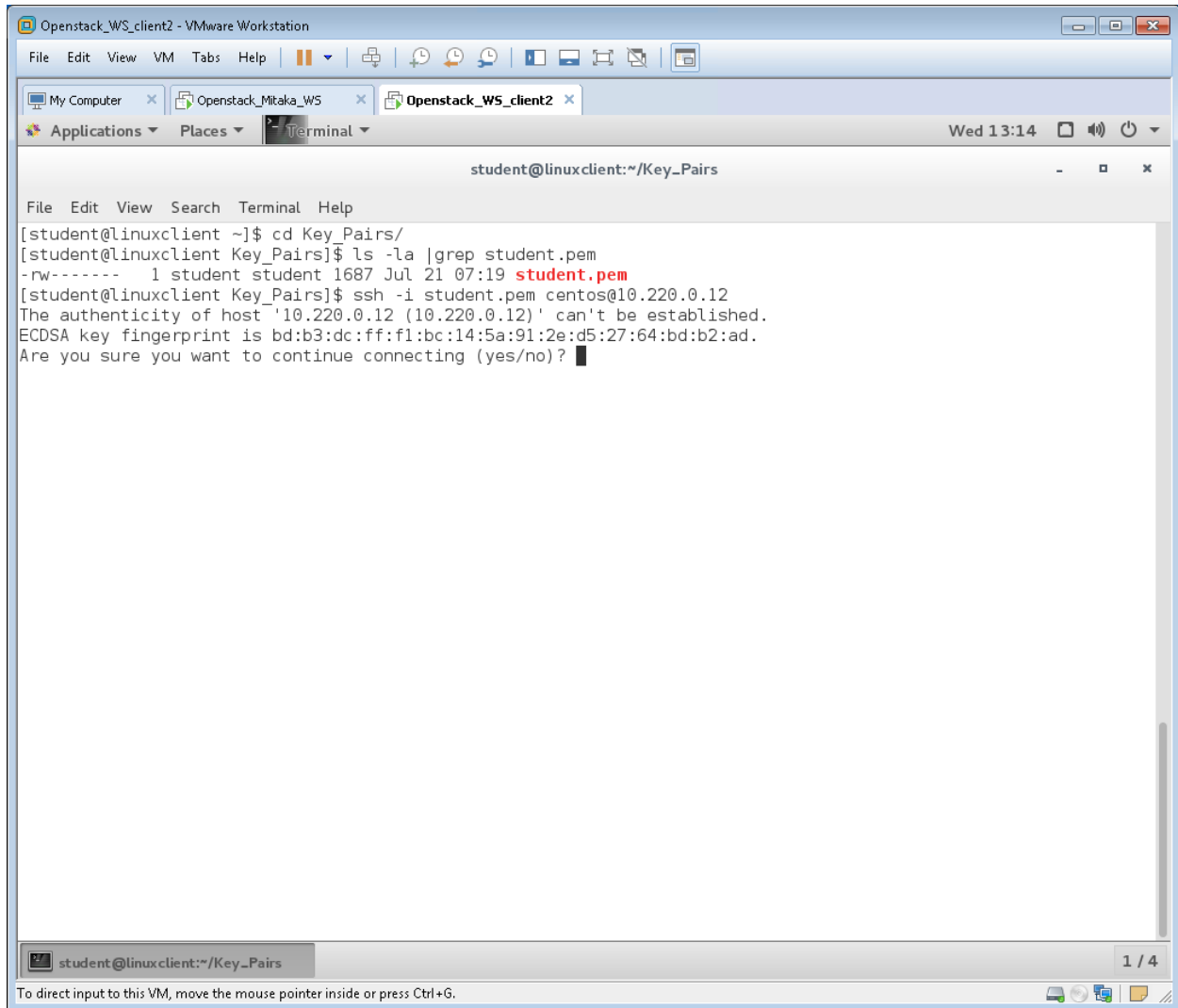
6. The result should be as pictured in the screen capture above. This is key pair that you moved with WinSCP in lab 6-1. **Verify** that the **student.pem permissions** are **-rw-----**, the key pair will not function if the permissions are not exactly as shown.

Note: If the permissions are not as shown above, you can fix this using the **chmod 600 student.pem** command from the Downloads working directory (not shown)

Note: The **chmod** is short for change file access permissions, and 600 is octal number string needed to change the student.pem file to read and write for the file owner only



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



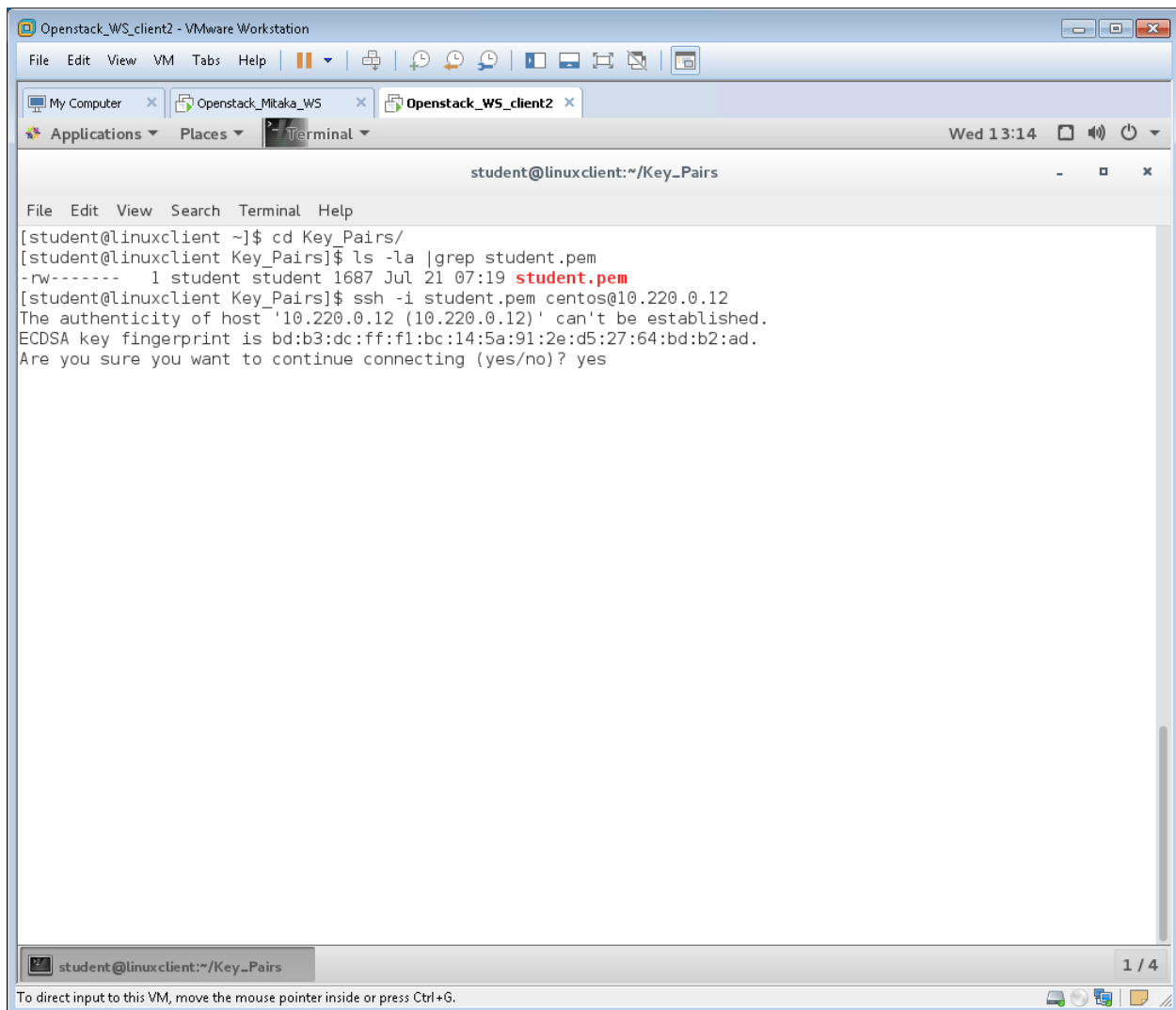
```
Openstack_WS_client2 - VMware Workstation
File Edit View VM Tabs Help
My Computer Openstack_Mitaka_WS Openstack_WS_client2
Applications Places Terminal
Wed 13:14
student@linuxclient:~/Key_Pairs
File Edit View Search Terminal Help
[student@linuxclient ~]$ cd Key_Pairs/
[student@linuxclient Key_Pairs]$ ls -la |grep student.pem
-rw----- 1 student student 1687 Jul 21 07:19 student.pem
[student@linuxclient Key_Pairs]$ ssh -i student.pem centos@10.220.0.12
The authenticity of host '10.220.0.12 (10.220.0.12)' can't be established.
ECDSA key fingerprint is bd:b3:dc:ff:f1:bc:14:5a:91:2e:d5:27:64:bd:b2:ad.
Are you sure you want to continue connecting (yes/no)?
```

7. Enter the command **ssh -i student.pem centos@10.220.0.12** and **press enter**.

Note: **ssh** is the command for secure remote login, **-i** is the identity file option, **centos** is the username for the remote machine, and the **@** symbol combines the username and IP address



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair

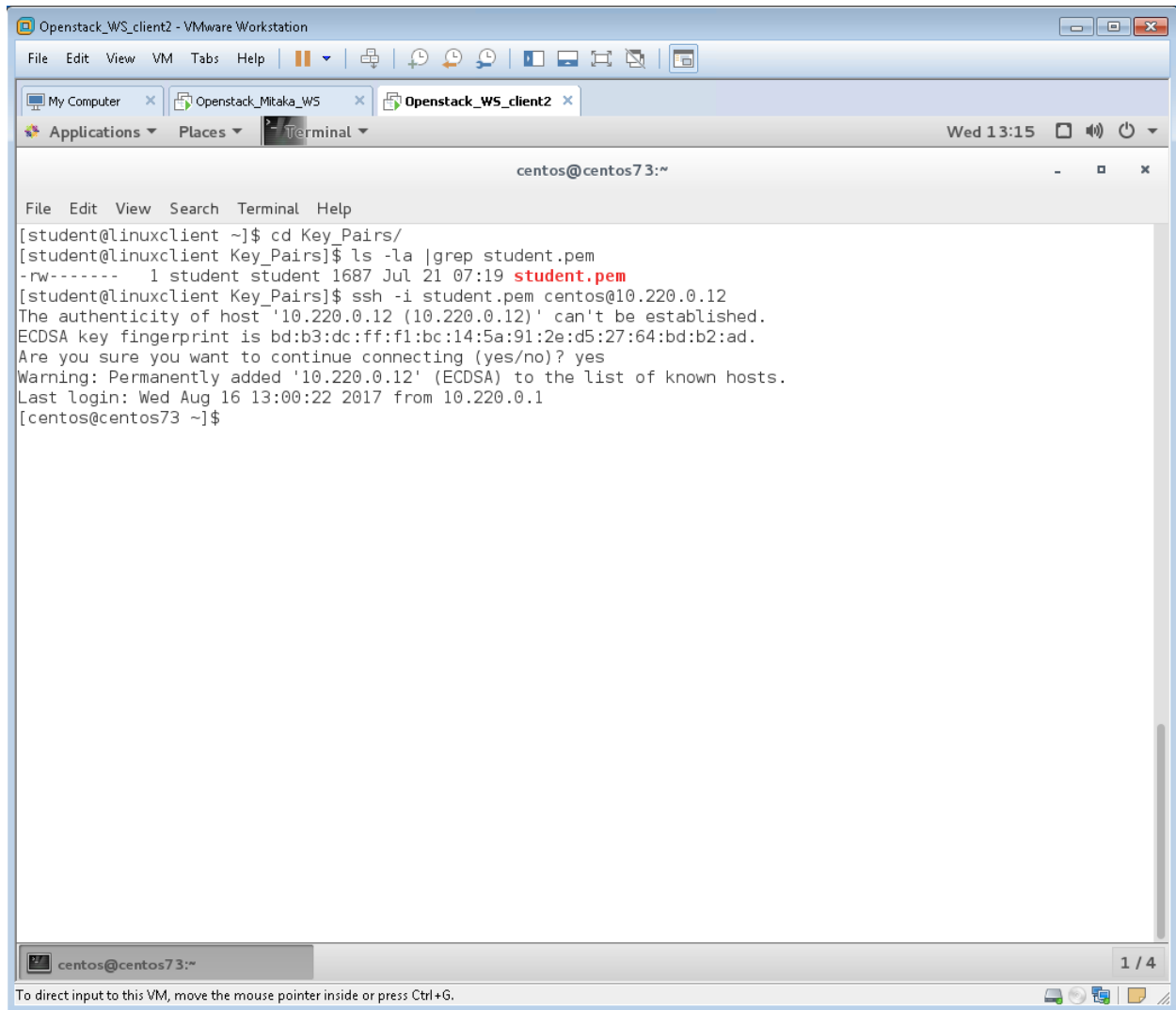


```
Openstack_WS_client2 - VMware Workstation
File Edit View VM Tabs Help
My Computer Openstack_Mitaka_W5 Openstack_WS_client2
Applications Places Terminal Wed 13:14
student@linuxclient:~/Key_Pairs
File Edit View Search Terminal Help
[student@linuxclient ~]$ cd Key_Pairs/
[student@linuxclient Key_Pairs]$ ls -la |grep student.pem
-rw----- 1 student student 1687 Jul 21 07:19 student.pem
[student@linuxclient Key_Pairs]$ ssh -i student.pem centos@10.220.0.12
The authenticity of host '10.220.0.12 (10.220.0.12)' can't be established.
ECDSA key fingerprint is bd:b3:dc:ff:f1:bc:14:5a:91:2e:d5:27:64:bd:b2:ad.
Are you sure you want to continue connecting (yes/no)? yes
```

8. Indicate that you want to continue connecting by typing **yes**



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



The screenshot shows a VMware Workstation window titled "Openstack_WS_client2 - VMware Workstation". Inside, there's a terminal window titled "centos@centos73:~". The terminal output shows the following commands and responses:

```
[student@linuxclient ~]$ cd Key_Pairs/
[student@linuxclient Key_Pairs]$ ls -la |grep student.pem
-rw----- 1 student student 1687 Jul 21 07:19 student.pem
[student@linuxclient Key_Pairs]$ ssh -i student.pem centos@10.220.0.12
The authenticity of host '10.220.0.12 (10.220.0.12)' can't be established.
ECDSA key fingerprint is bd:b3:dc:ff:f1:bc:14:5a:91:2e:d5:27:64:bd:b2:ad.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.220.0.12' (ECDSA) to the list of known hosts.
Last login: Wed Aug 16 13:00:22 2017 from 10.220.0.1
[centos@centos73 ~]$
```

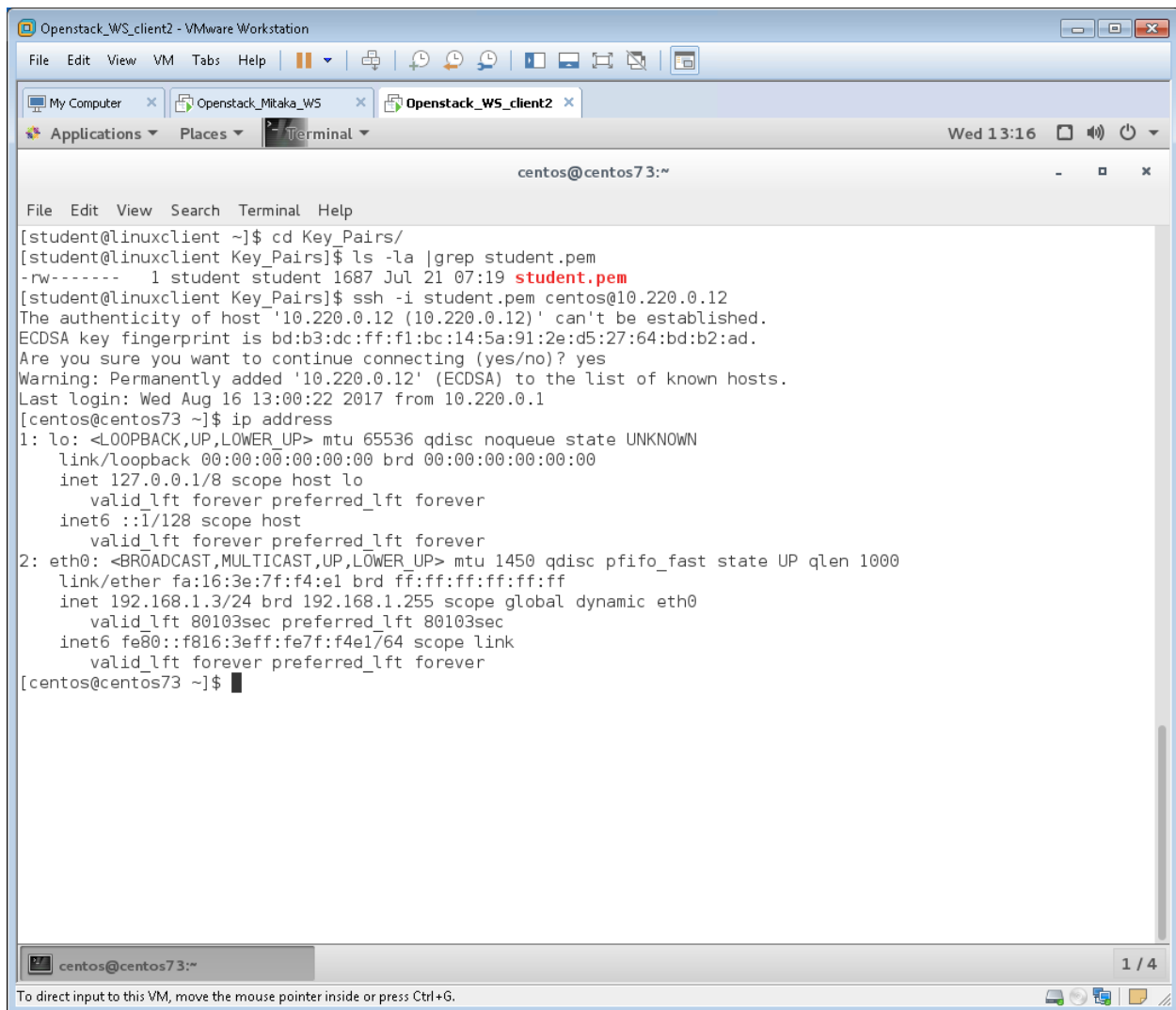
The terminal window also shows a status bar at the bottom with the text "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

9. If you see something similar to the above screen capture, you have successfully “remoted” into the CentOS7#3 instance.

Note: You may have noticed the Last login: information is displayed and that the username and hostname changed from “**student@linuxclient**” to “**centos@centos73**”



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



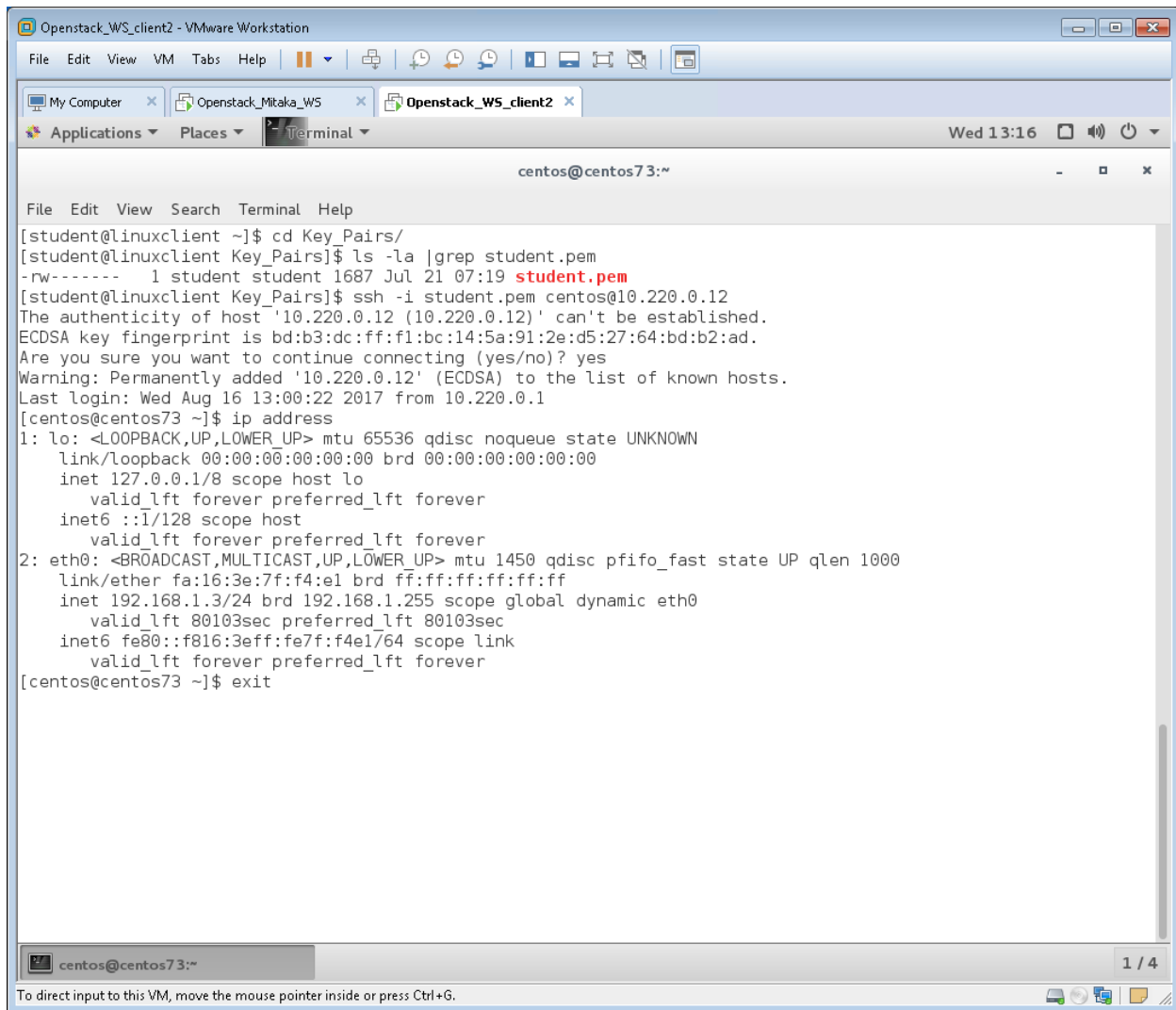
```
Openstack_WS_client2 - VMware Workstation
File Edit View VM Tabs Help
My Computer Openstack_Mitaka_W5 Openstack_WS_client2
Applications Places Terminal Wed 13:16

centos@centos73:~
File Edit View Search Terminal Help
[student@linuxclient ~]$ cd Key_Pairs/
[student@linuxclient Key_Pairs]$ ls -la | grep student.pem
-rw----- 1 student student 1687 Jul 21 07:19 student.pem
[student@linuxclient Key_Pairs]$ ssh -i student.pem centos@10.220.0.12
The authenticity of host '10.220.0.12 (10.220.0.12)' can't be established.
ECDSA key fingerprint is bd:b3:dc:ff:f1:bc:14:5a:91:2e:d5:27:64:bd:b2:ad.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.220.0.12' (ECDSA) to the list of known hosts.
Last login: Wed Aug 16 13:00:22 2017 from 10.220.0.1
[centos@centos73 ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:7f:f4:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 80103sec preferred_lft 80103sec
    inet6 fe80::f816:3eff:fe7f:f4e1/64 scope link
        valid_lft forever preferred_lft forever
[centos@centos73 ~]$
```

10. Type **ip address** press Enter. You should see the same output as you did when the running the command from the PuTTY terminal window from the Windows VM



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



The screenshot shows a VMware Workstation window titled "Openstack_WS_client2 - VMware Workstation". Inside, there's a terminal window titled "centos@centos73:~". The terminal shows the following commands and output:

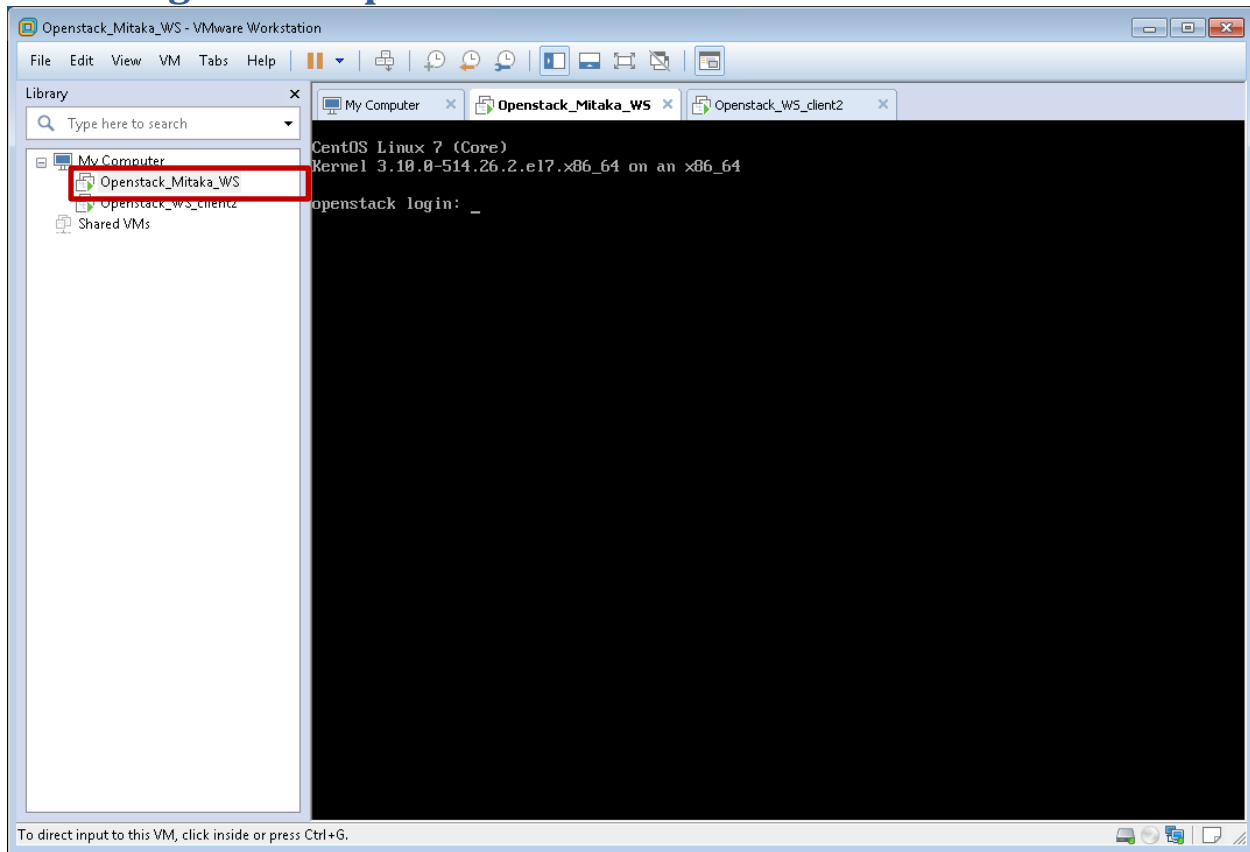
```
[student@linuxclient ~]$ cd Key_Pairs/
[student@linuxclient Key_Pairs]$ ls -la |grep student.pem
-rw----- 1 student student 1687 Jul 21 07:19 student.pem
[student@linuxclient Key_Pairs]$ ssh -i student.pem centos@10.220.0.12
The authenticity of host '10.220.0.12 (10.220.0.12)' can't be established.
ECDSA key fingerprint is bd:b3:dc:ff:f1:bc:14:5a:91:2e:d5:27:64:bd:b2:ad.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.220.0.12' (ECDSA) to the list of known hosts.
Last login: Wed Aug 16 13:00:22 2017 from 10.220.0.1
[centos@centos73 ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:7f:f4:e1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 80103sec preferred_lft 80103sec
    inet6 fe80::f816:3eff:fe7f:f4e1/64 scope link
        valid_lft forever preferred_lft forever
[centos@centos73 ~]$ exit
```

11. Type **exit** and press **enter** to end the connection to the remote machine centos7

Continue to grade script



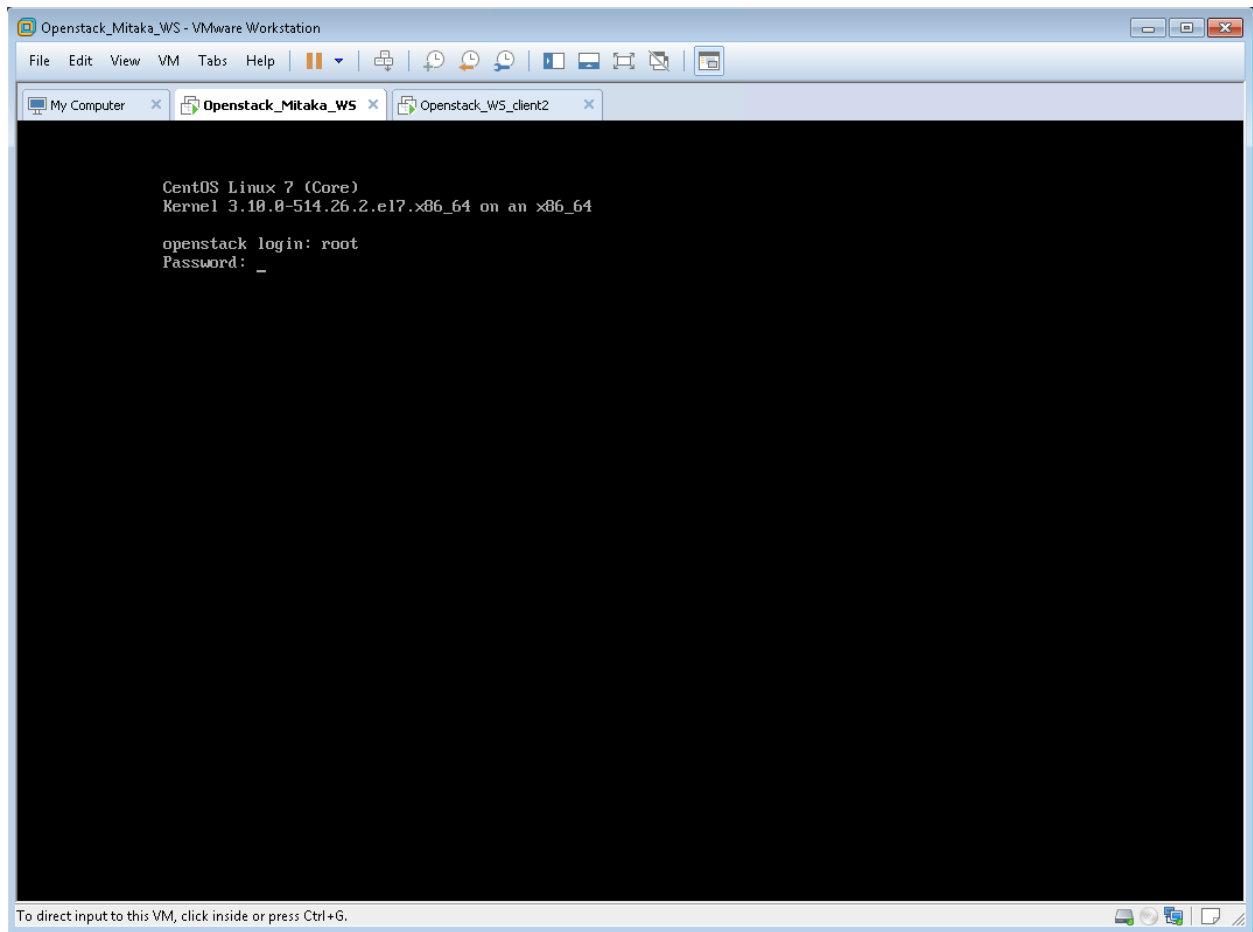
Run the grade script



1. Return to Workstation and **Click on OpenStack_Mitaka_WS VM.**

Note: The OpenStack_Mitaka_WS console may still be open on your desktop from when you ran the setup script

Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair

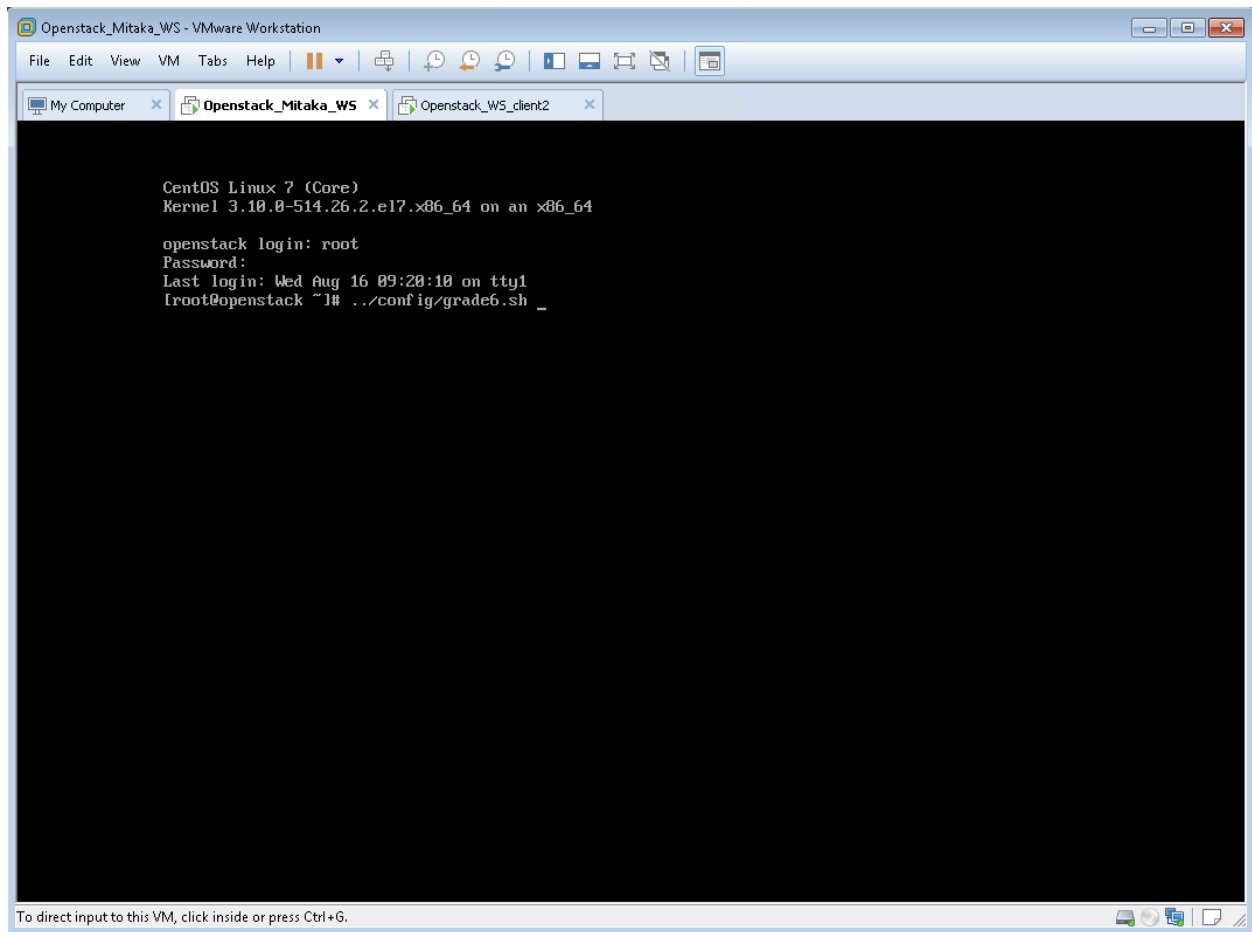


2. Log in as root with the Password: P@ssword

Note: The password is NOT visible as you type it



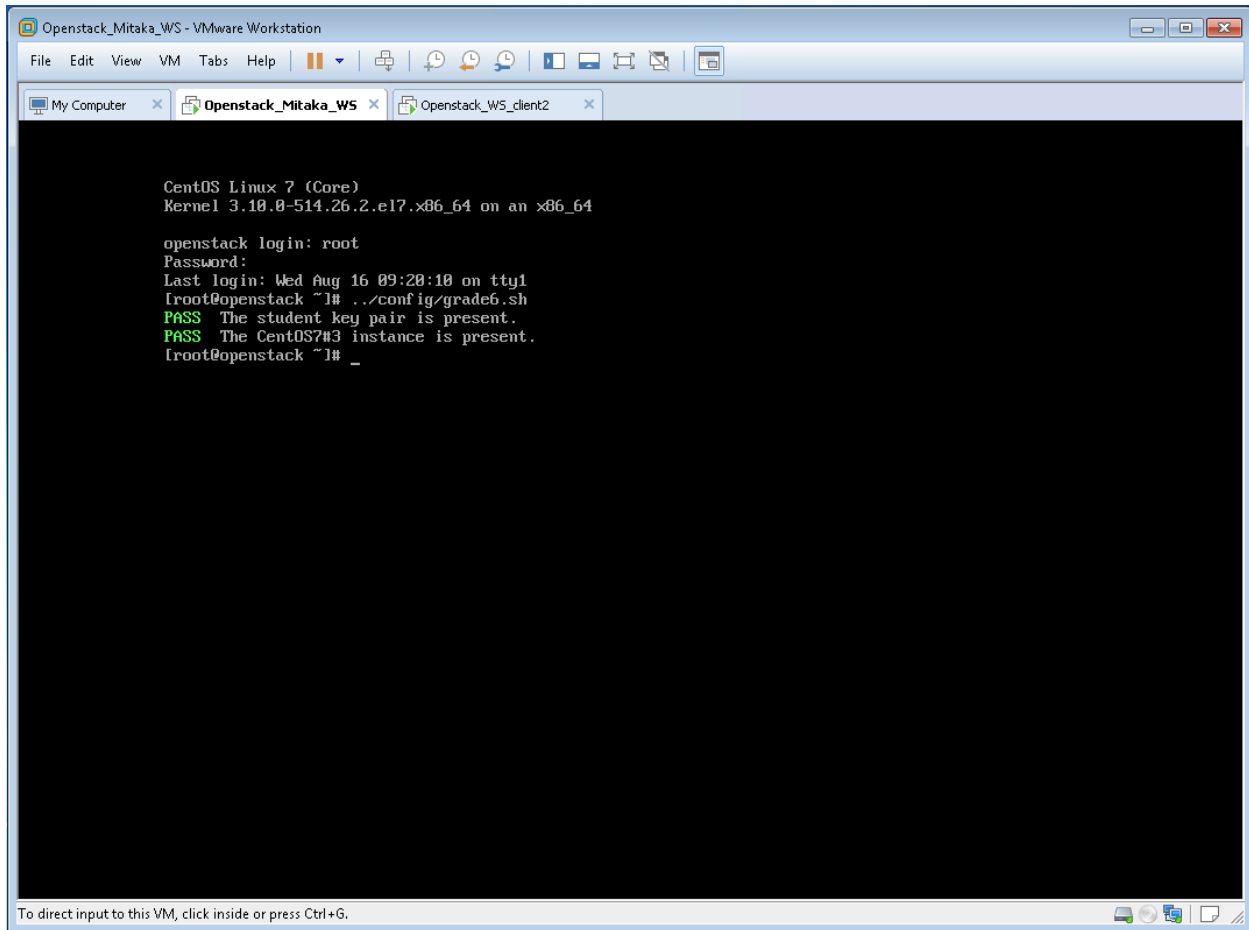
Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



3. Enter the command; `../config/grade6.sh` and **press Enter**



Module 6: Manage Key Pairs and Connect to an Instance using a Key Pair



```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.2.el7.x86_64 on an x86_64

openstack login: root
Password:
Last login: Wed Aug 16 09:20:10 on tty1
[root@openstack ~]# ../config/grade6.sh
PASS The student key pair is present.
PASS The CentOS7#3 instance is present.
[root@openstack ~]# _
```

4. The grading script will produce an output with **PASS** or **FAIL** for each of the categories, similar to the screen capture above. If you receive a **FAIL** on one or more of the categories, you can go back and fix the issue and run the grading script again, or you can revert the OpenStack_Mitaka_WS VM to the base snapshot and start over again.

This completes Module 6, continue to conclusion



Conclusion:

You have successfully assisted the customer in using various techniques to manager their private key pair, how to use PuTTY to connect to their CentOS 7instance from a Windows machine, and using the Linux command line to SSH into their CentOS 7 instance. During your next field visit you will assist the customer in launching a Windows instance and use remote desktop to connect to their Windows instance.

