|  |  |
| --- | --- |
| IST198  OpenStack  Administration | Version 1: 2017-08-16 |
| These exercises will guide the student through the concepts and topics learned in chapter 4, upload a Key Pair, manage security groups and rules, and allocate a floating IP address in OpenStack Mitaka installed on CentOS 7. | Upload Key Pair, add Security Group & Rules, Allocate Floating IP Address. |

**Attributions:**

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

C:\Users\ronaldsharman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\OpenStack_Logo_Horizontal.eps 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 7

Run the Lab setup script 8

Access the OpenStack Dashboard 12

Lab 11: Import a Key Pair 15

Lab 12: Create a Security Group and Rules 27

Lab 13: Allocate a Floating IP Address 39

Run the Lab grade script 45

Conclusion 49

**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:**

* Import a public key pair into OpenStack, Create a Security Group and Rules, and allocate a floating IP address to an instance.

**Labs 11-13**

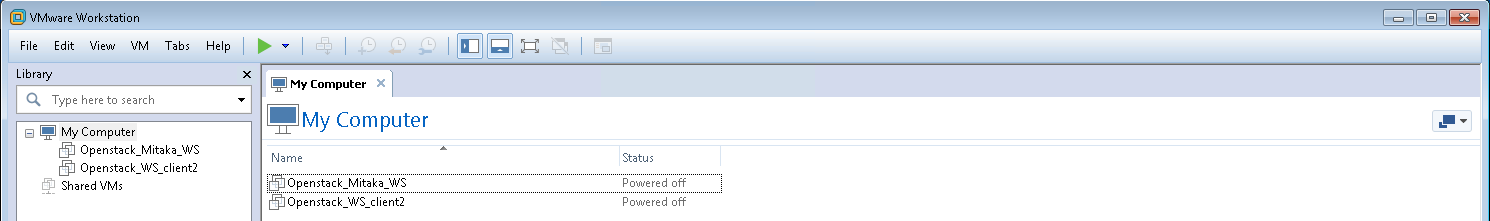
This lab will guide the student through importing a public key pair, creating a Security Group and Rules, and add a Floating IP address to an OpenStack project using the OpenStack Dashboard.

**(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).**

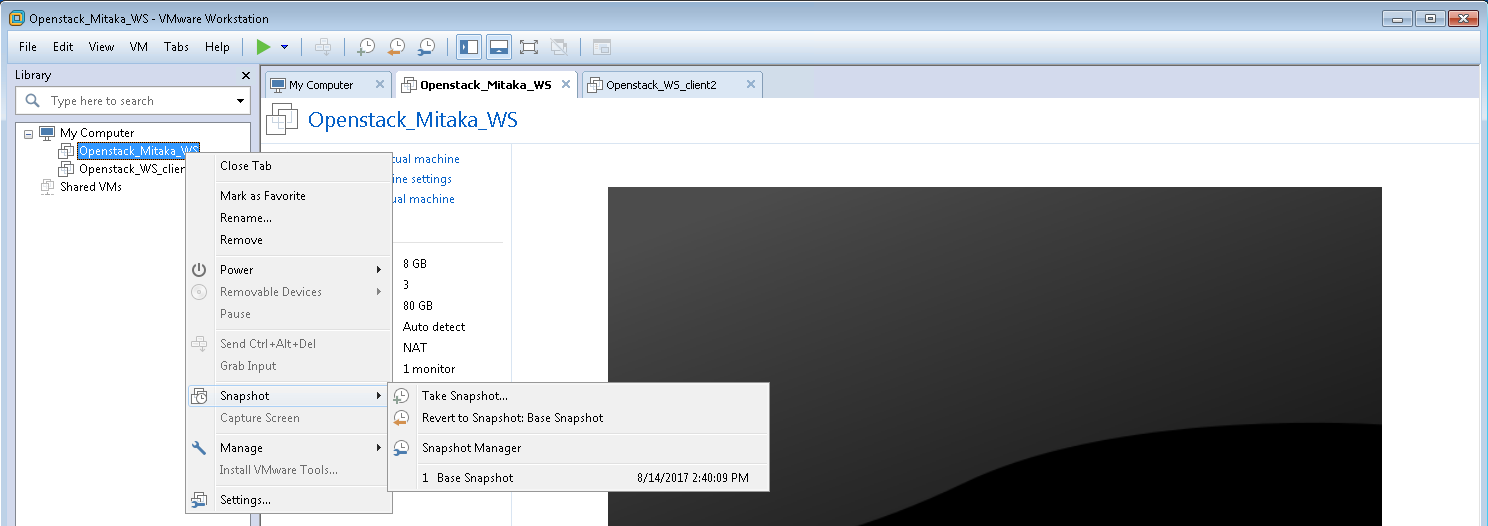
**Prepare the OpenStack Virtual Machines**



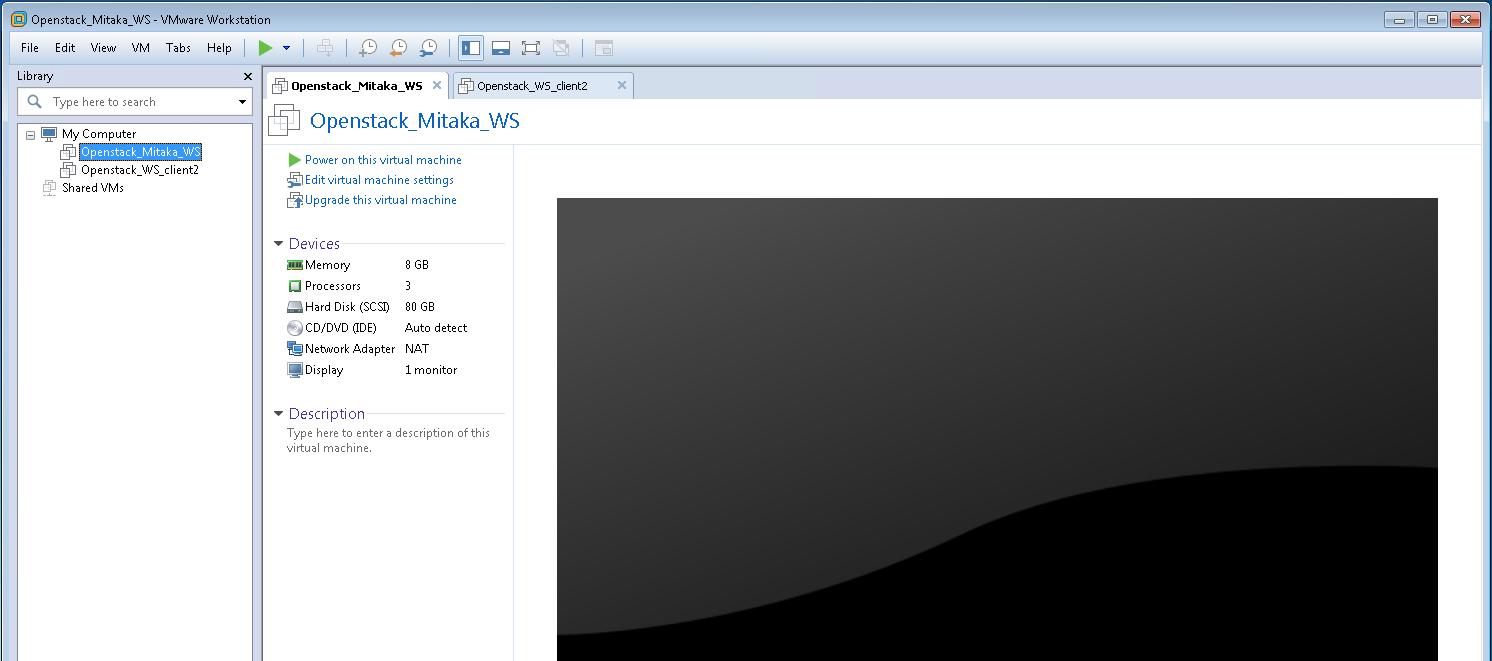
1. **Launch** the **VMware Workstation Pro application**



1. Workstation should have two virtual machines (VM) installed; Openstack\_Mitaka\_WS and Openstack\_WS\_client2.

****

1. 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.

****

1. **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 importing a public key pair to their project, create a security group and rules to allow inbound SSH and ICMP network traffic, and assign a Floating IP to their CentOS7#2 cloud instance using the OpenStack Dashboard.

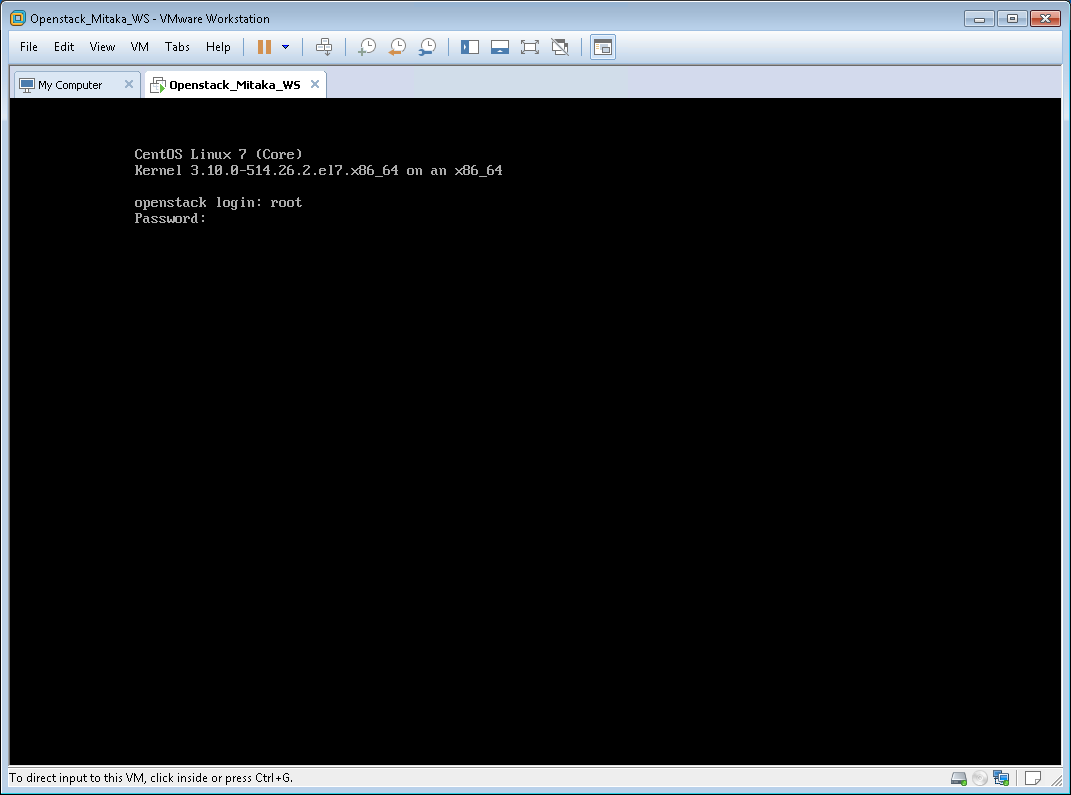
**Lab Settings**

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 |

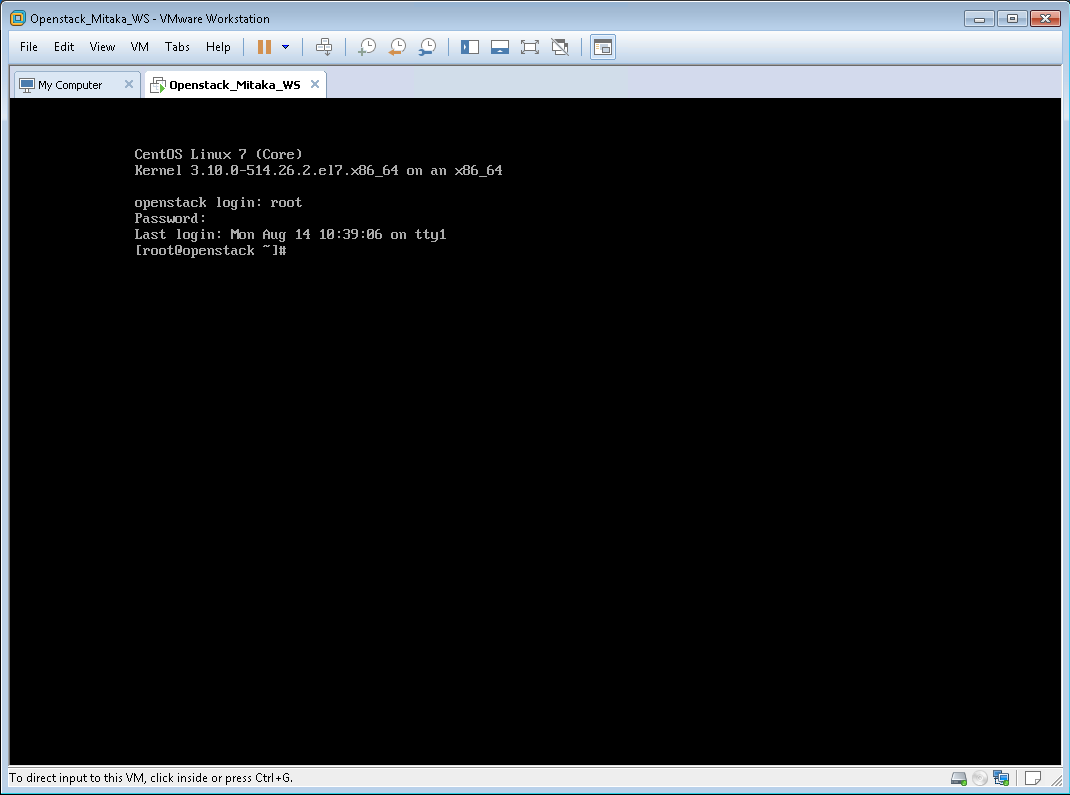
Note: In this OpenStack VMware Workstation environment, the two VMs can be reverted back to their base snapshot at any time. This means that you can explore or experiment without fear of permanently damaging the OpenStack environment. If you make a mistake that you can’t recover from, then stop and revert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

**Run the lab setup script**

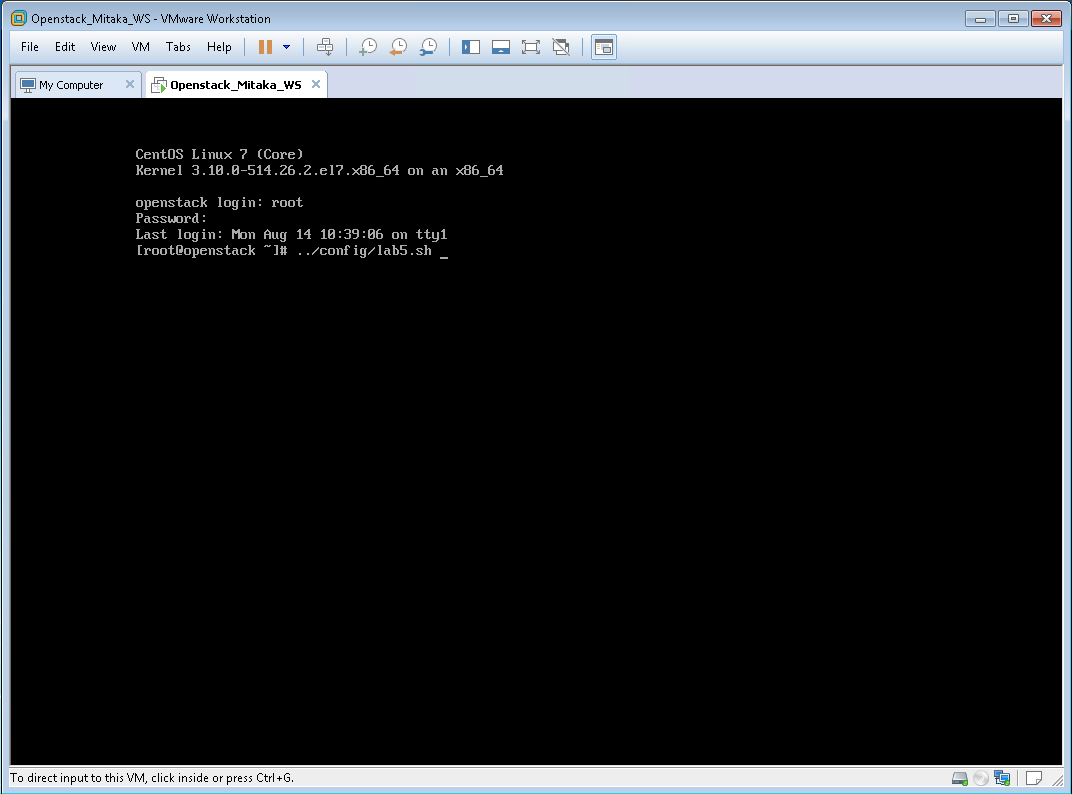
****

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

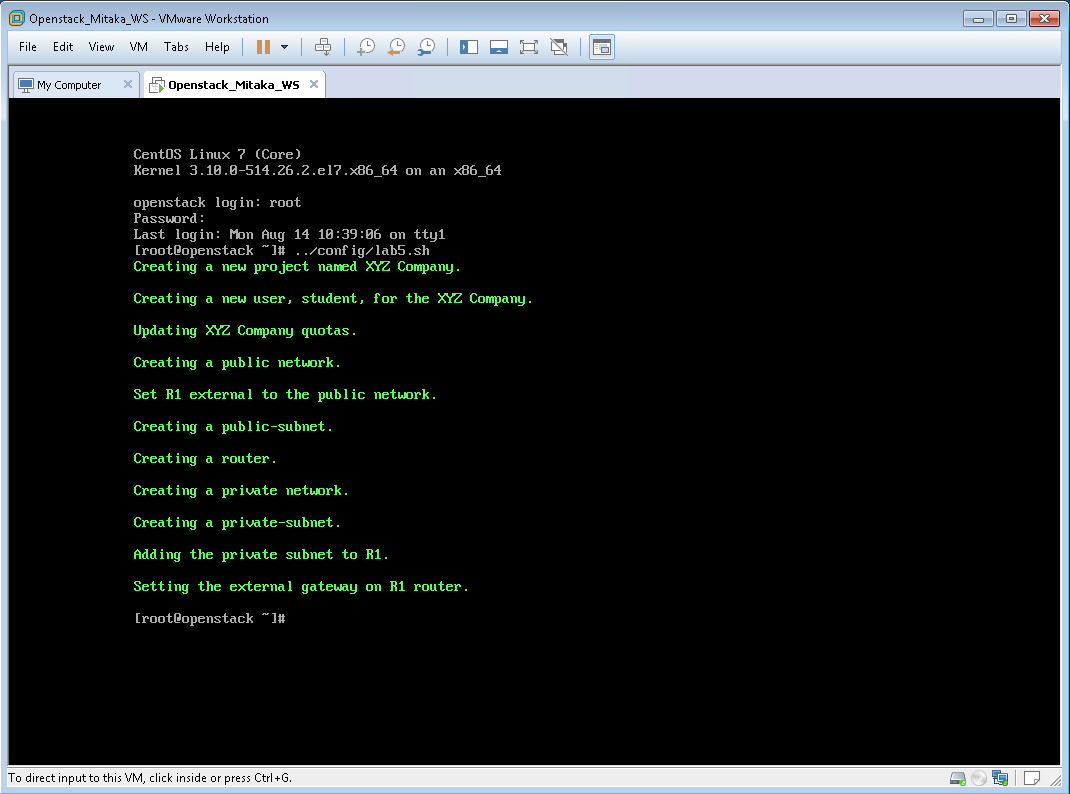
Note: The password is NOT visible as you type it

****

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

****

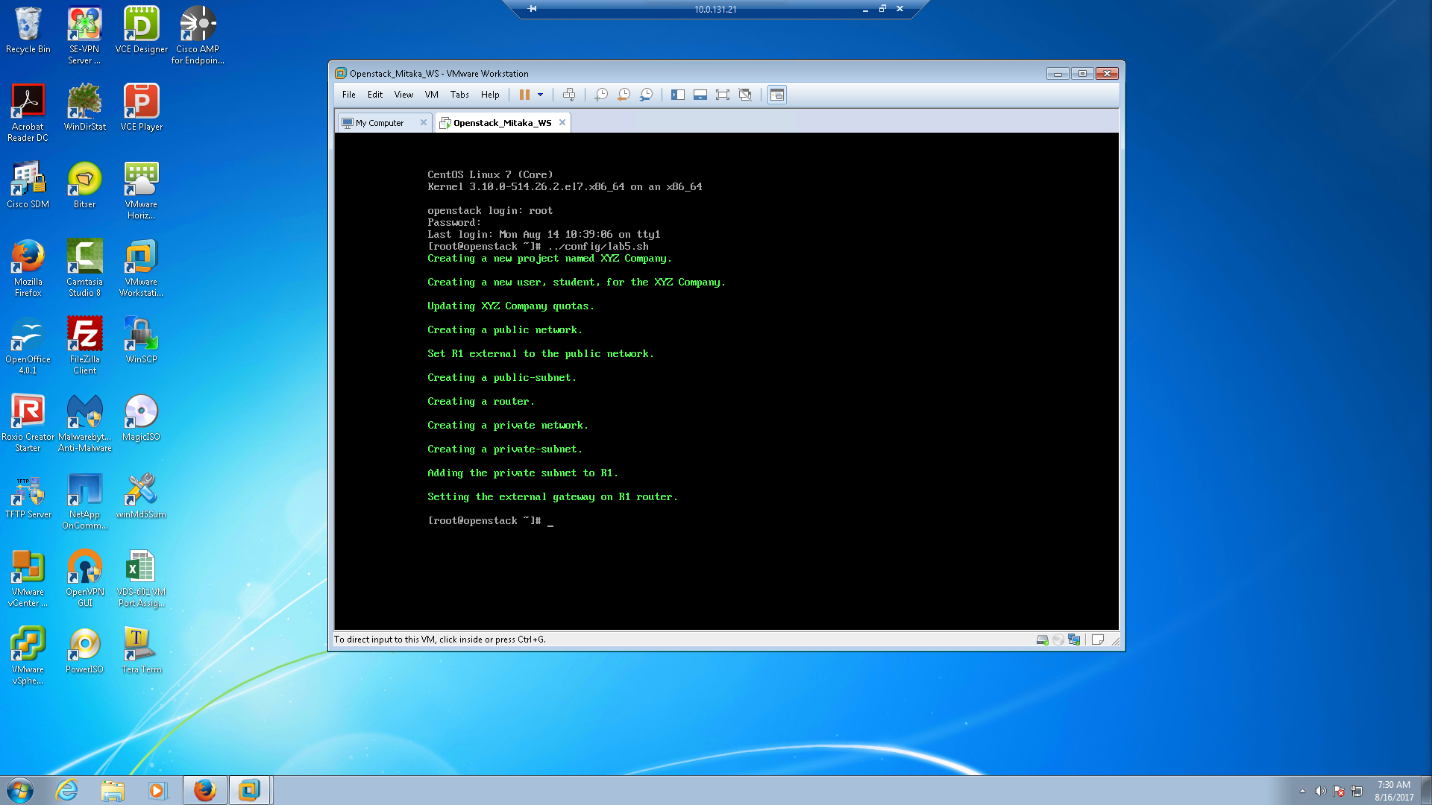
1. Type the command; **../config/lab5.sh** and **press Enter** as shown in the screen capture above to run the Module 5 setup script



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

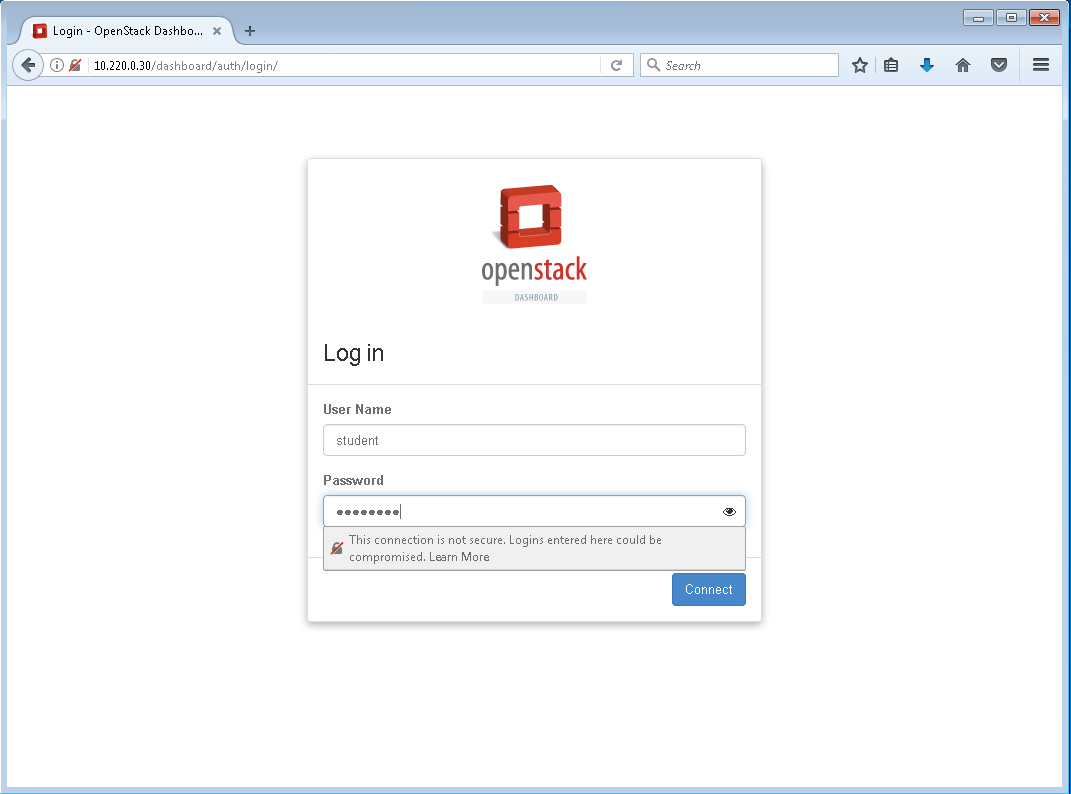
Note: The script is complete when the **[root@openstack ~]#** prompt returns

**Access the OpenStack Dashboard**

****

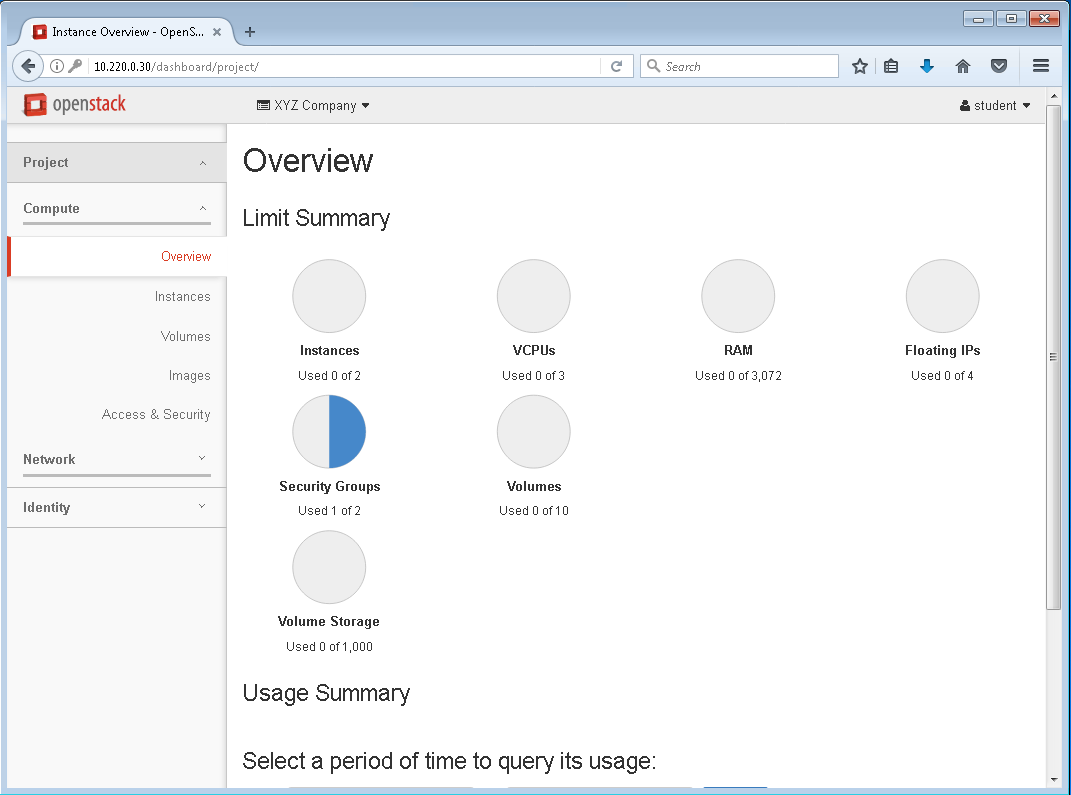
1. On your Windows host PC, open an internet browser

Note: Openstack\_mitaka\_client2 is a CentOS 7 desktop VM that you can use as an alternate to the Windows host PC to accomplish all of the labs, unless specifically noted in the instructions.

****

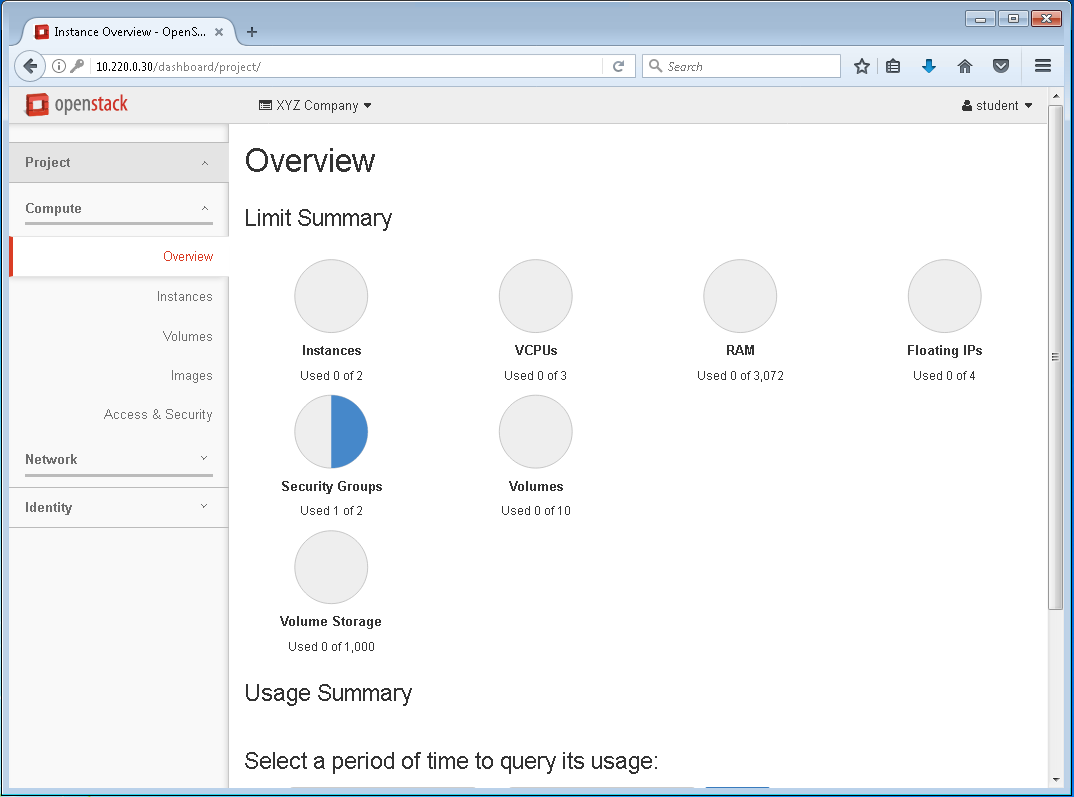
1. **Navigate** to **http://10.220.0.30/dashboard. Login** to the OpenStack Dashboard with the username **student** and **P@ssword** and press **enter** or **click Connect**

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



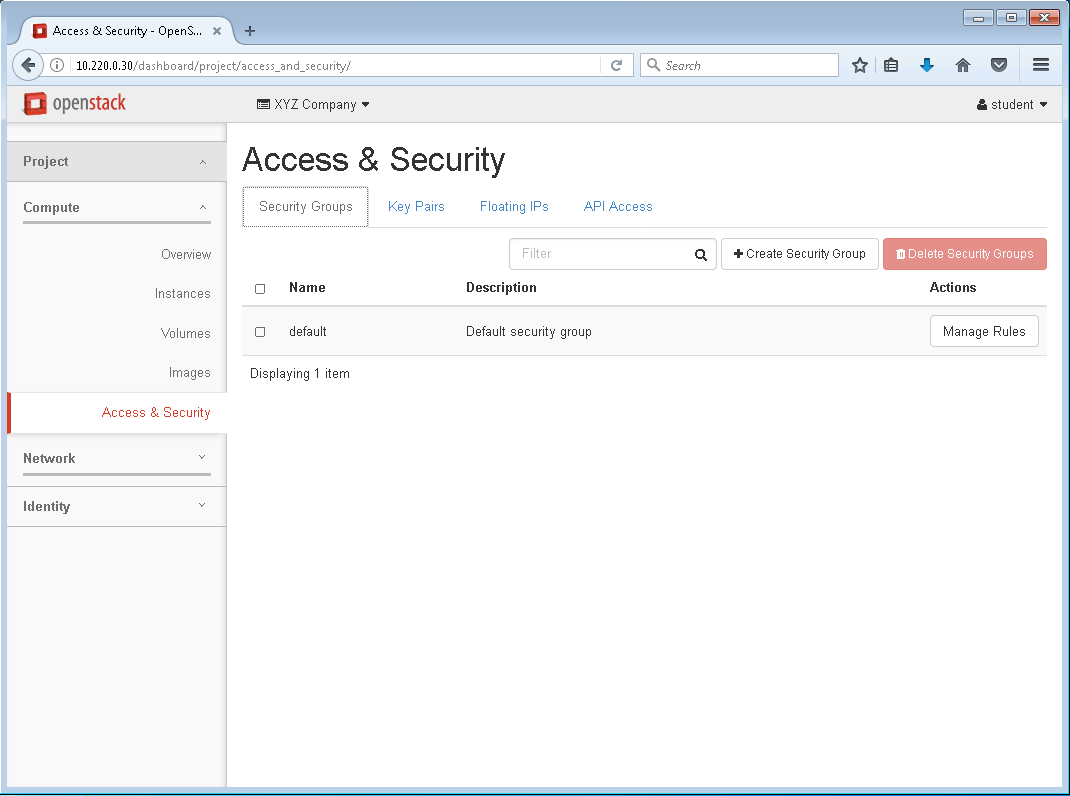
1. This is the homepage of the OpenStack Dashboard as seen from the XYZ Companies’ customer perspective.

**Lab 11: Import a Key Pair**

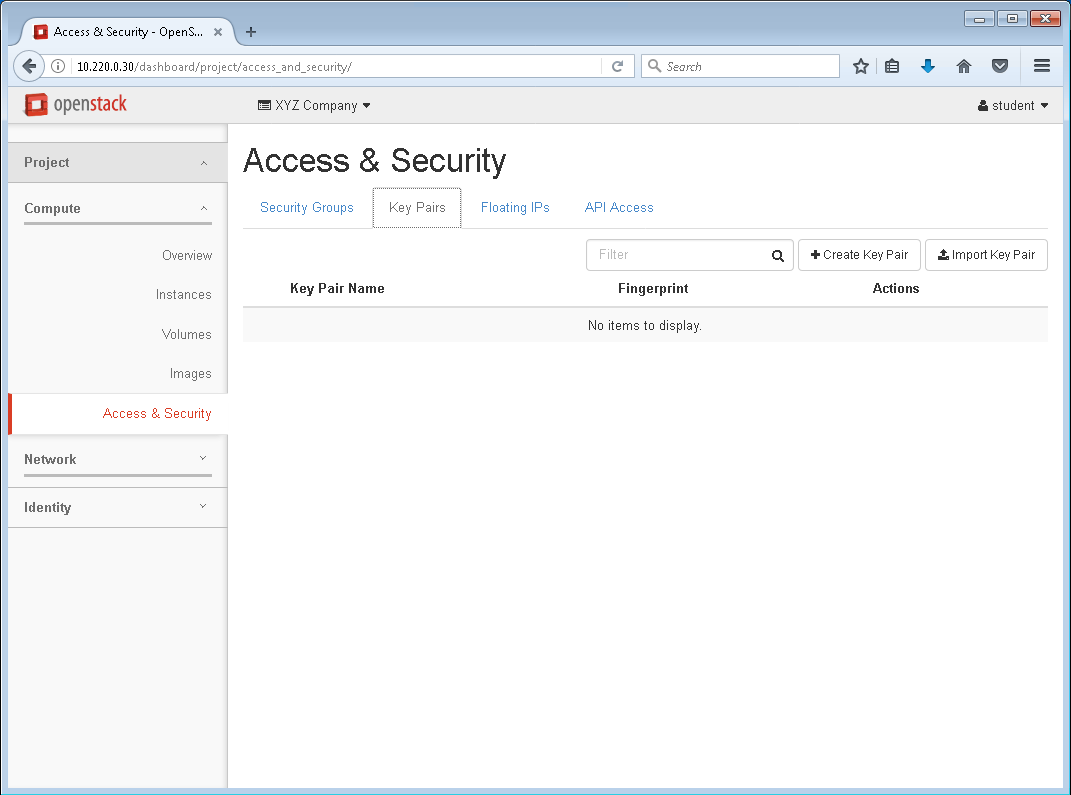
****

1. **Click** on **Access & Security**

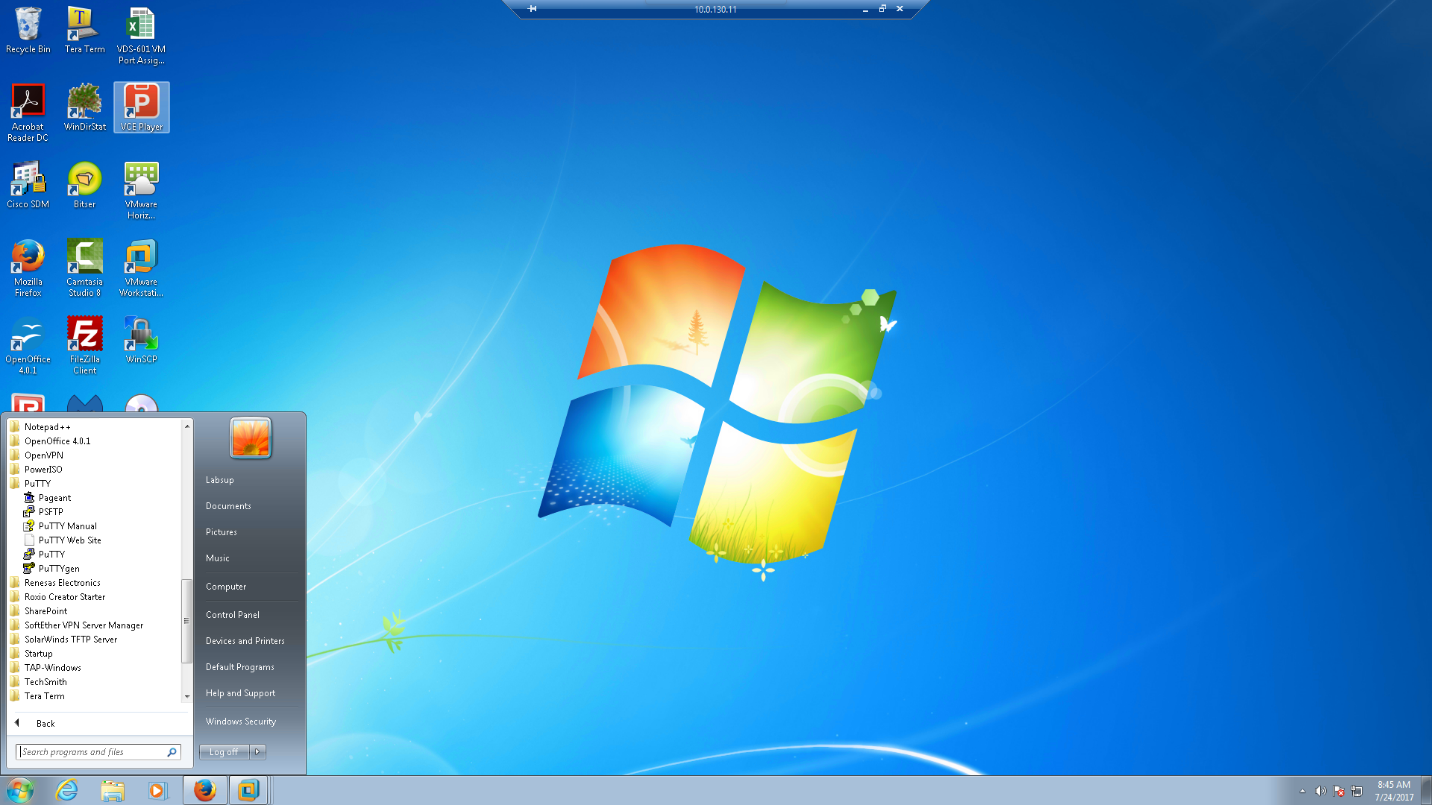
Note: This lab assumes that the student Key Pair, from previous labs, is present in your host downloads folder. If you don’t have the Key Pair in the host downloads folder, create a new Key Pair named student.pem and save it to the host downloads folder and resume Lab 11.



1. **Click** on the **Key Pairs** tab

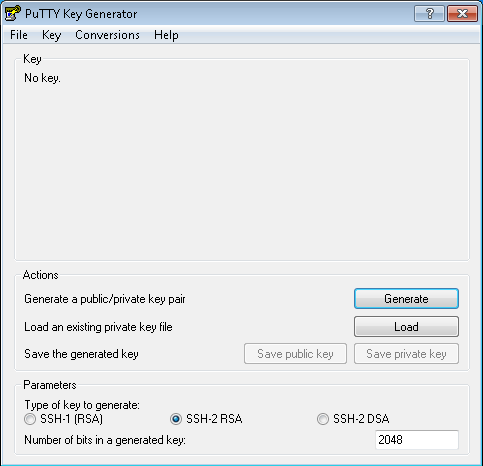


1. **Minimize** the **OpenStack web page**

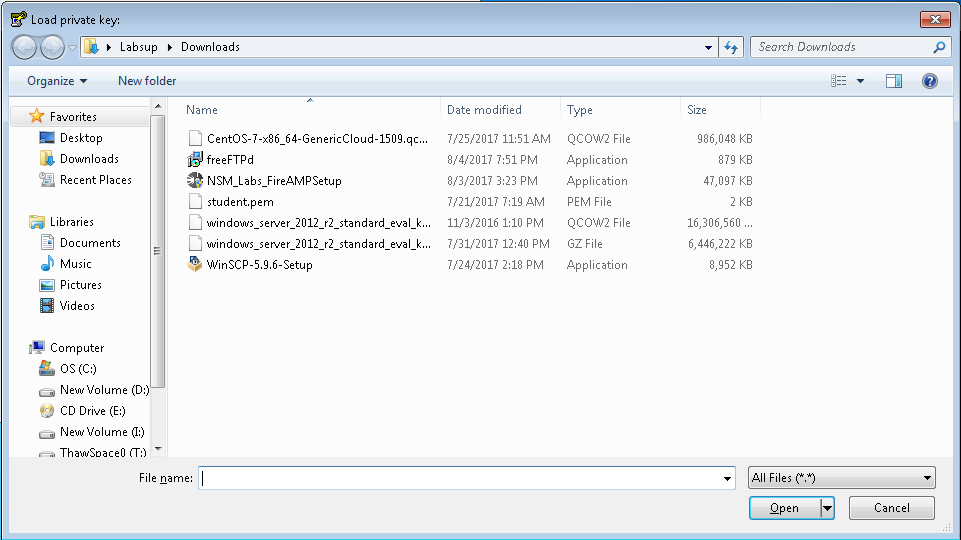


1. **Open PuTTY Key Generator** All Programs>PuTTY>PuTTYgen

Note: Representative image, your host will be different.

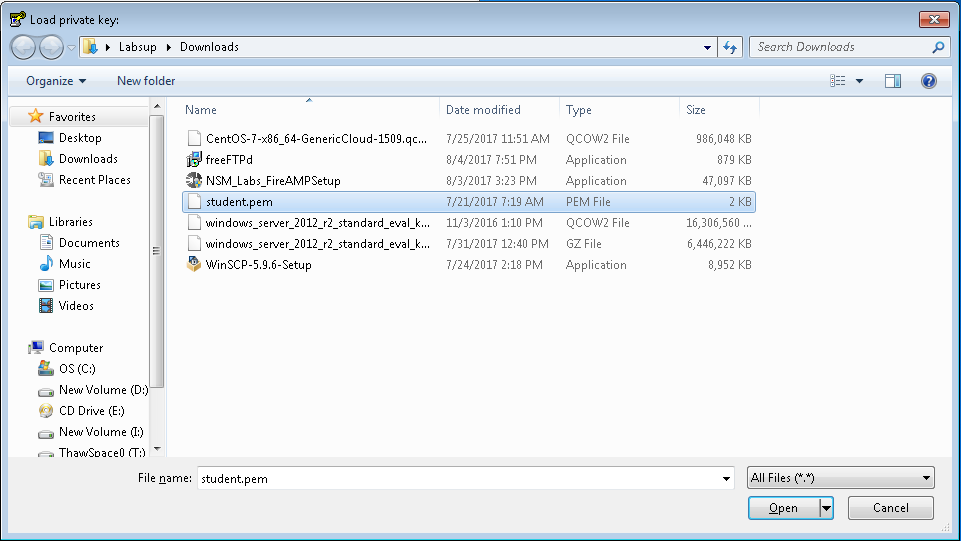


1. **Click** on **Load**

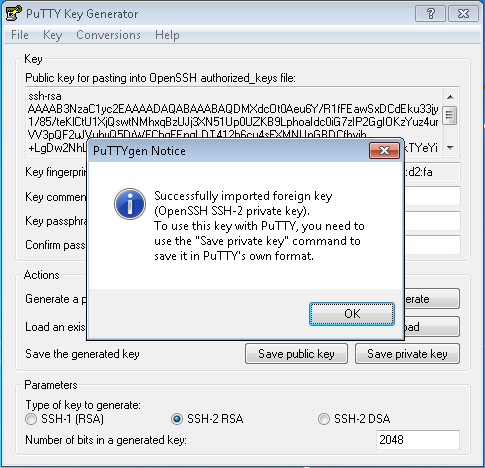


1. Using the drop down menu, **select All Files (\*.\*)**

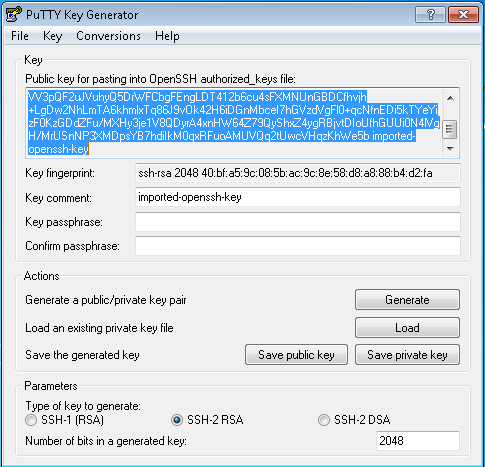
Note: Representative image, your host downloads folder will not contain the same items.



1. **Select** the **student PEM File**, **click open**



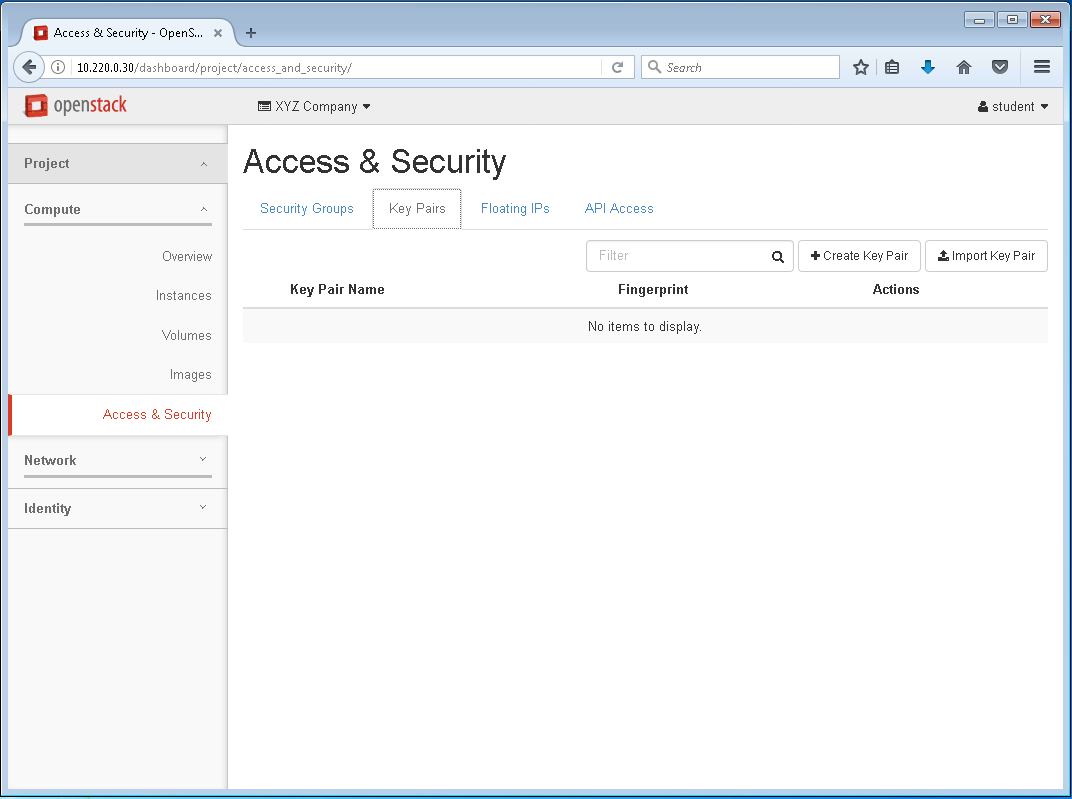
1. **Click OK** to proceed



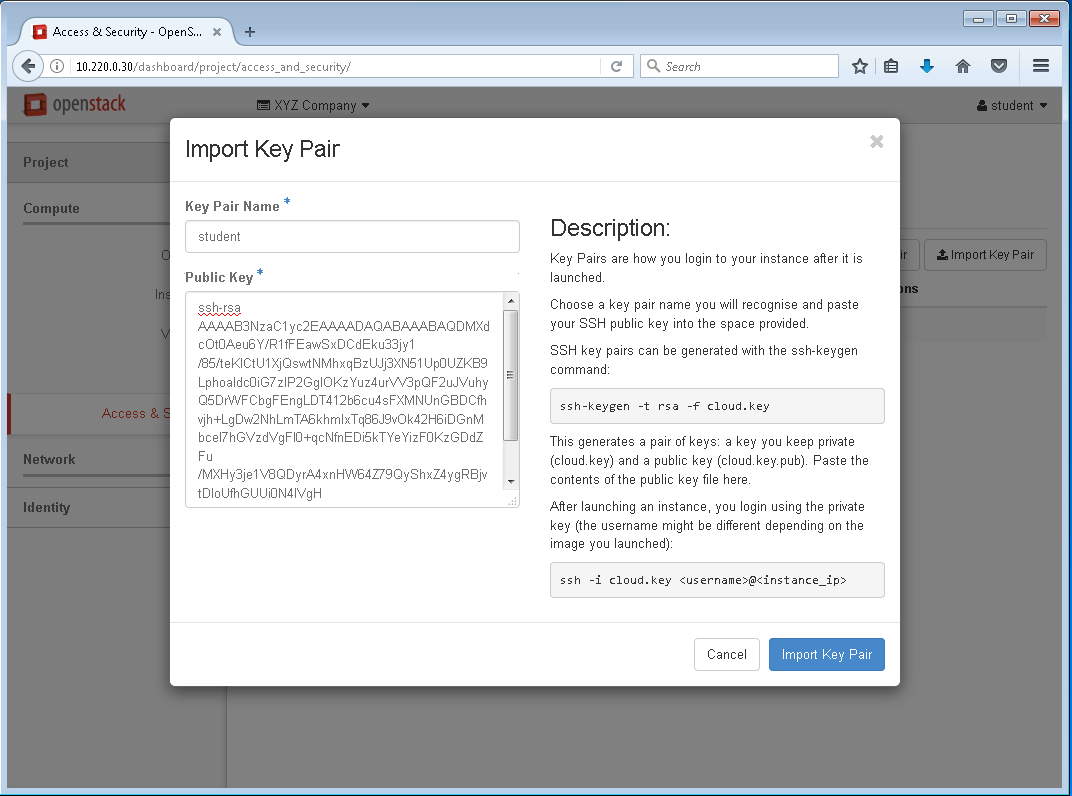
1. **Highlight** and **copy** the **Public key for pasting into OpenSSH authorized\_keys file:** as shown in the screen capture.

Note: Use the right click and copy feature on your mouse

Note: Ensure that you capture the entire key. It begins with ssh-rsa and ends with imported-openssh-key. Your public key information will be different then this screenshot.



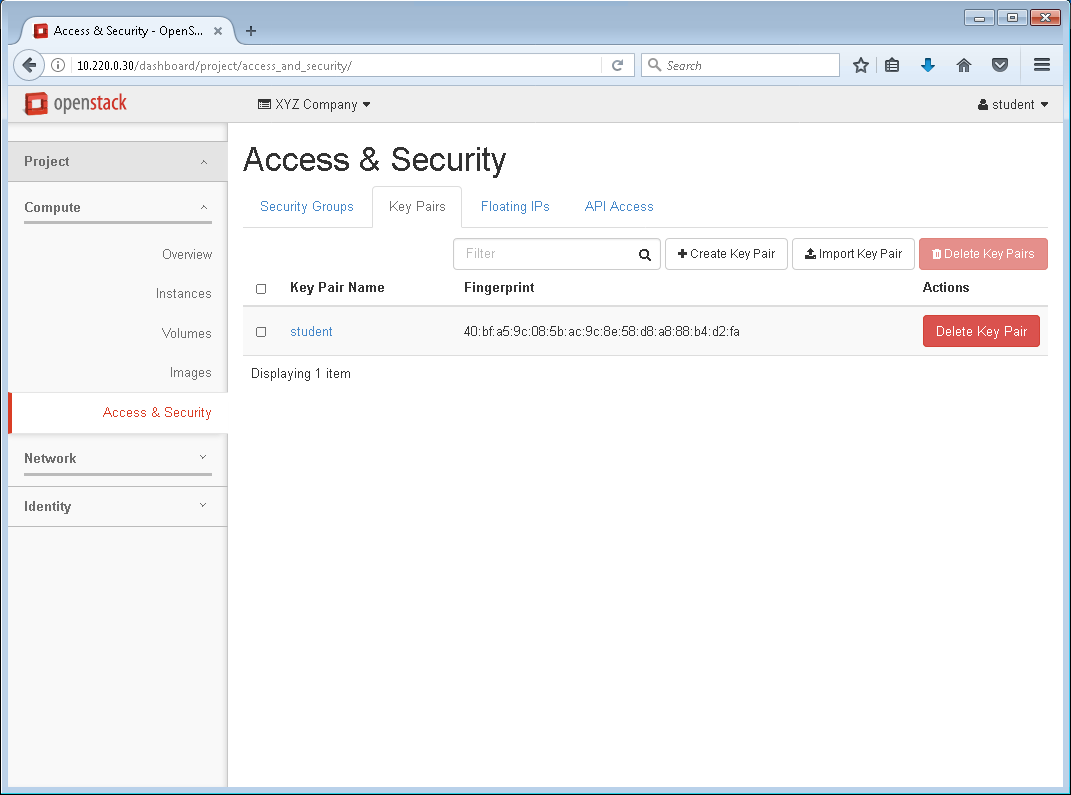
1. Return to the OpenStack web page and **click** on **Import Key Pair**



1. **Enter student** in the Key Pair Name block and **paste** what you copied into the Public Key block. **Click** on **Import Key Pair**

Note: Use the right click and paste feature on your mouse.

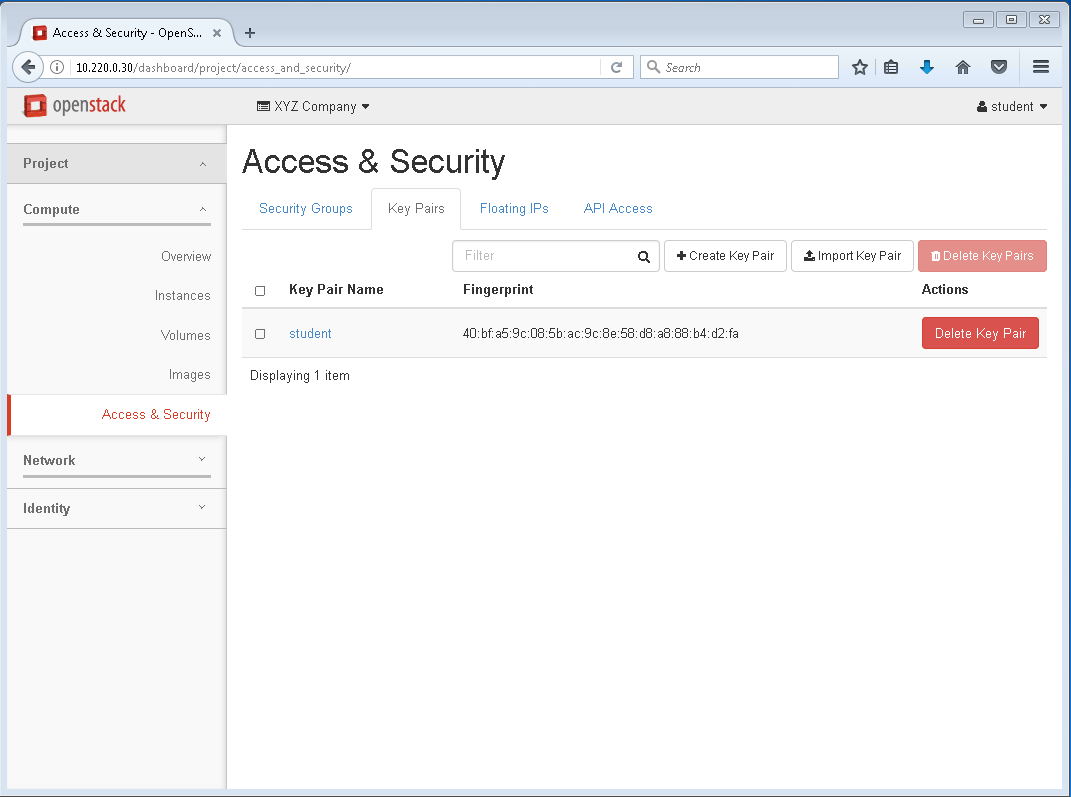
Note: Make sure that you have copied all of the public key; it begins with **ssh-rsa** and ends with **imported-openssh-key**



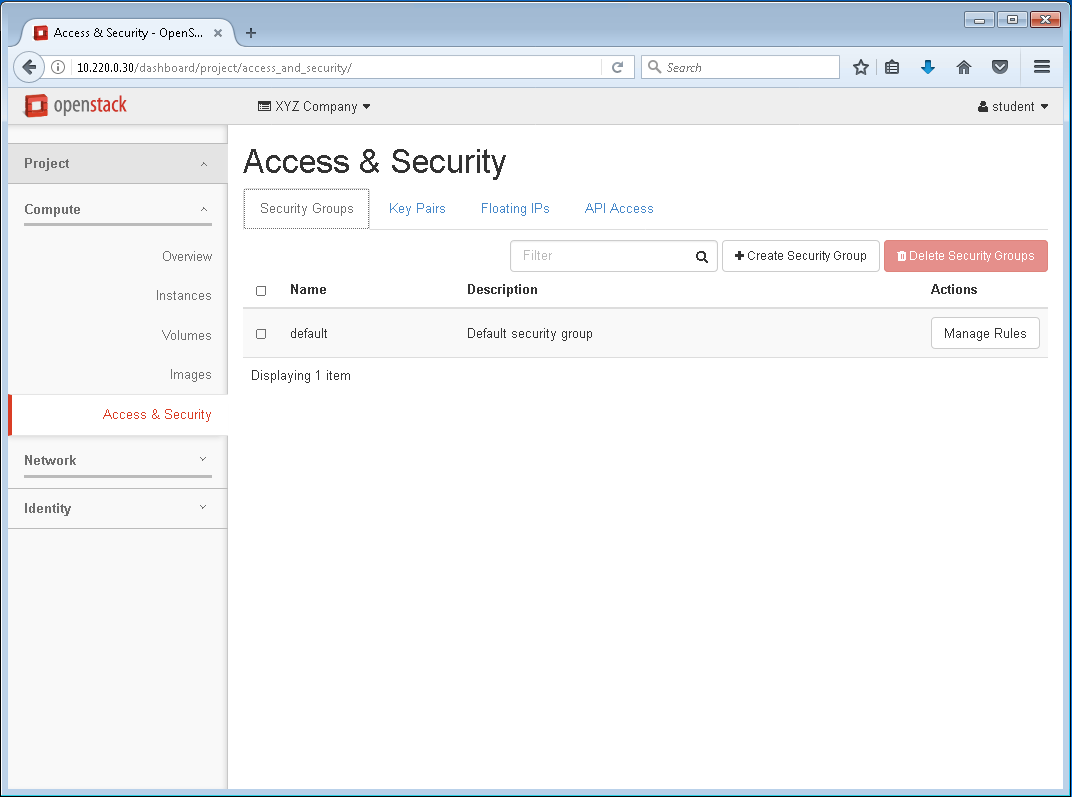
1. The student Key Pair should successfully import as shown in the screen capture above

Continue to Lab 12

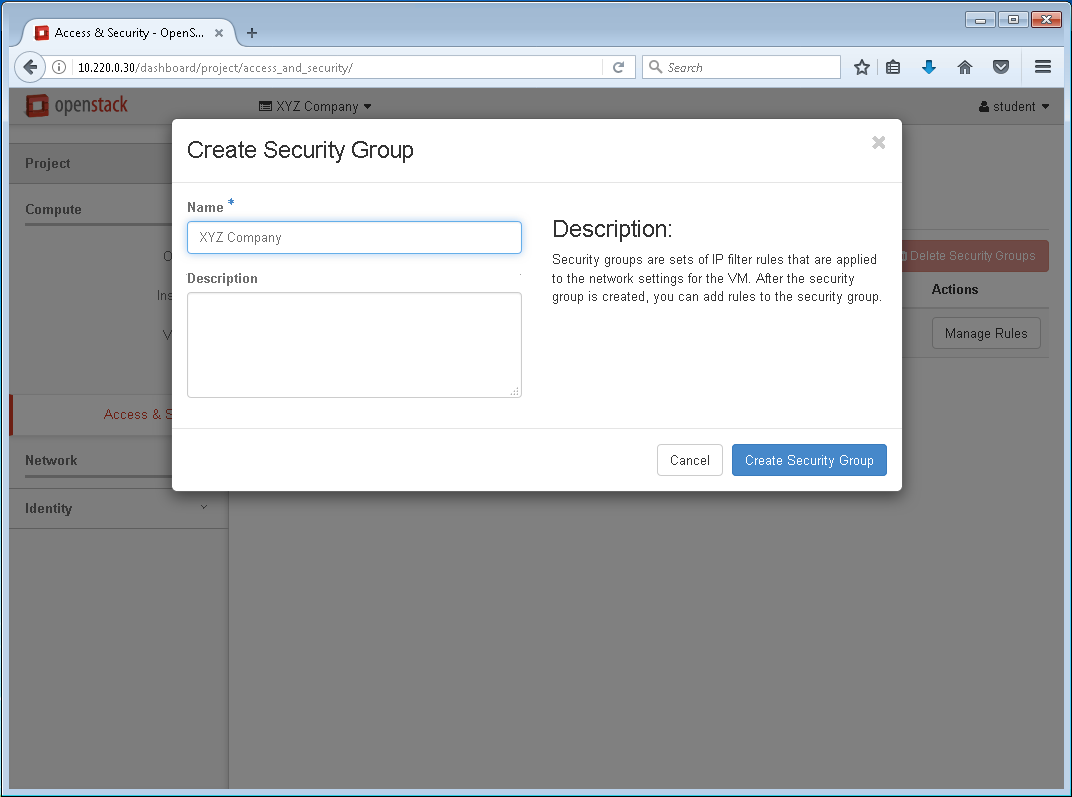
**13: Create a Security Group**

****

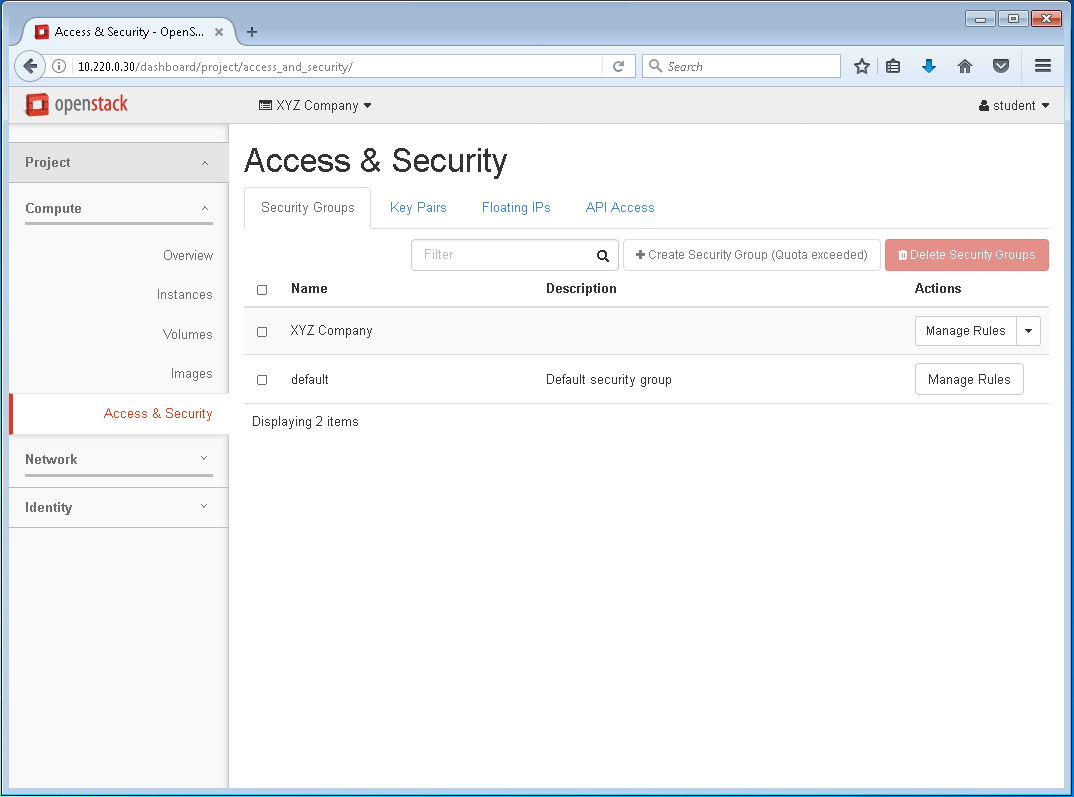
1. **Click** on **Security Groups**



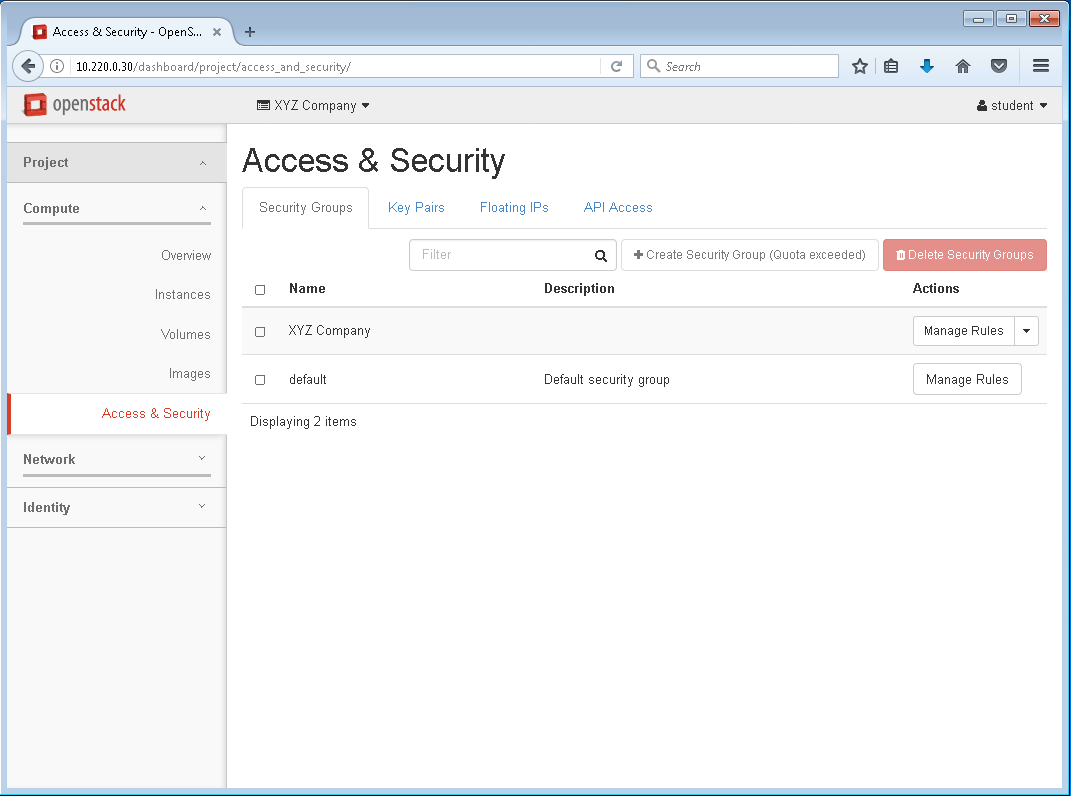
1. **Click** on **Create Security Group**



1. **Enter XYZ Company** in the Name block, **Click Create Security Group**



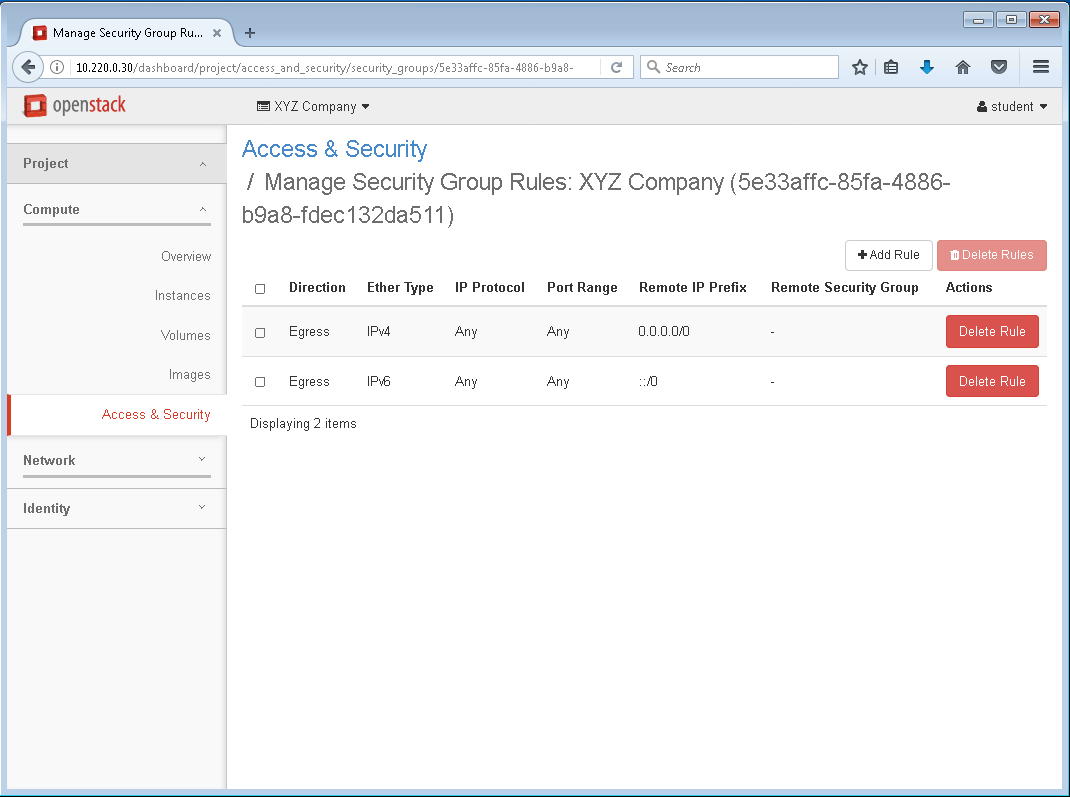
1. The XYZ Company should be added as shown



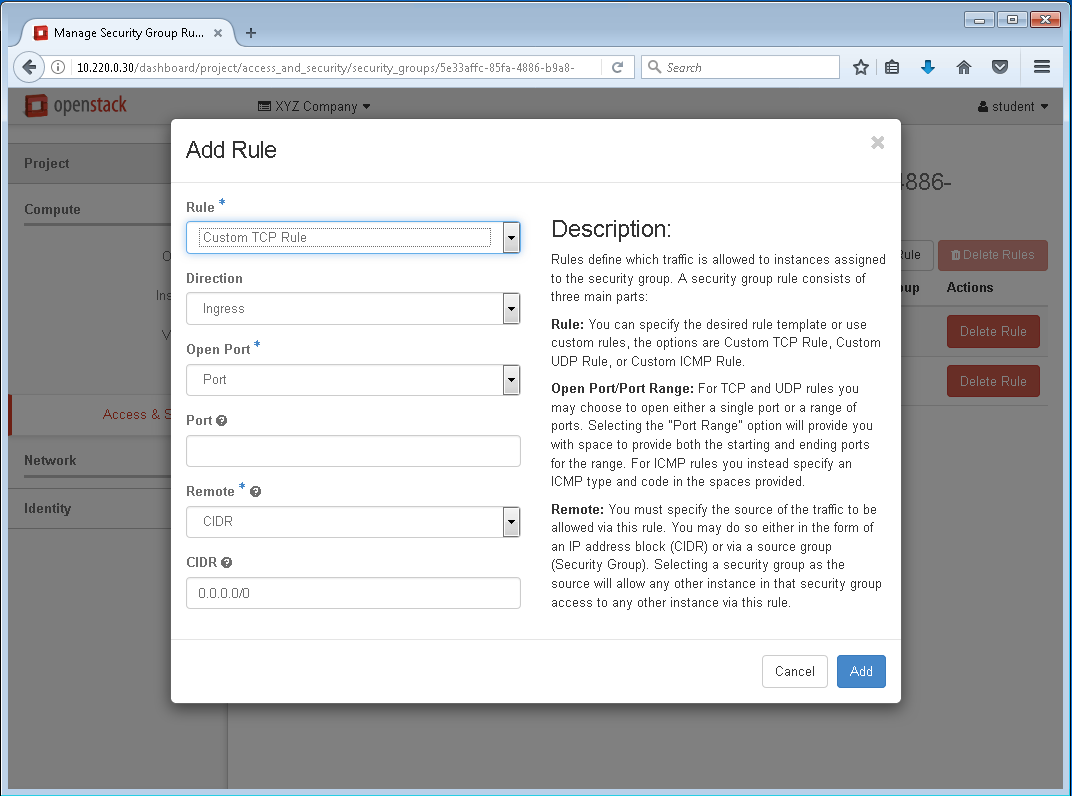
1. **Click** on **Manage Rules** for the XYZ Company security group

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.



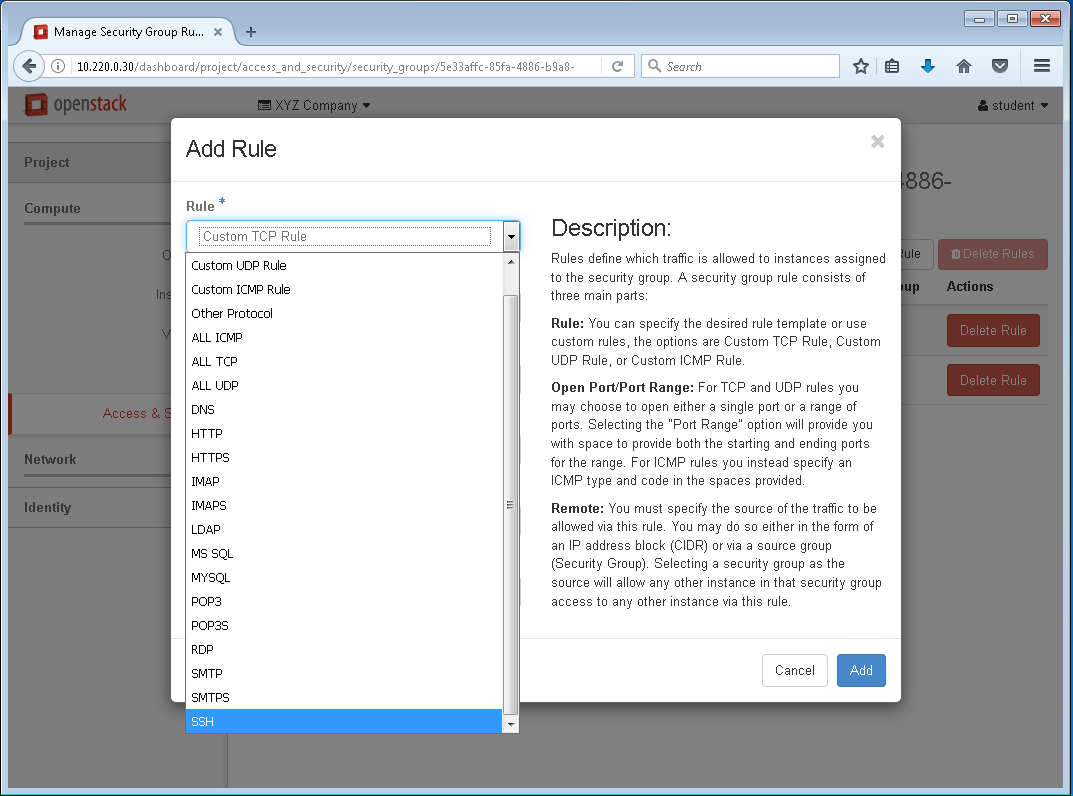
1. **Click** on **Add Rule**



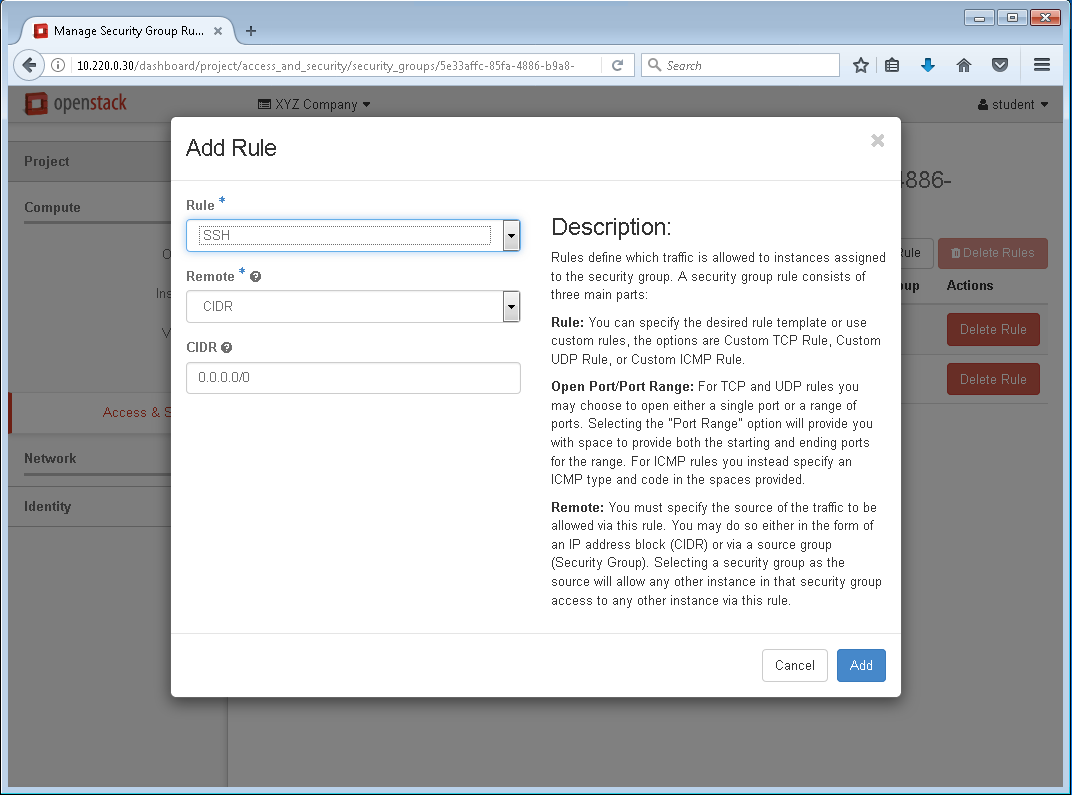
1. **Select** the **dropdown menu** for Rule.

Security Group Rules

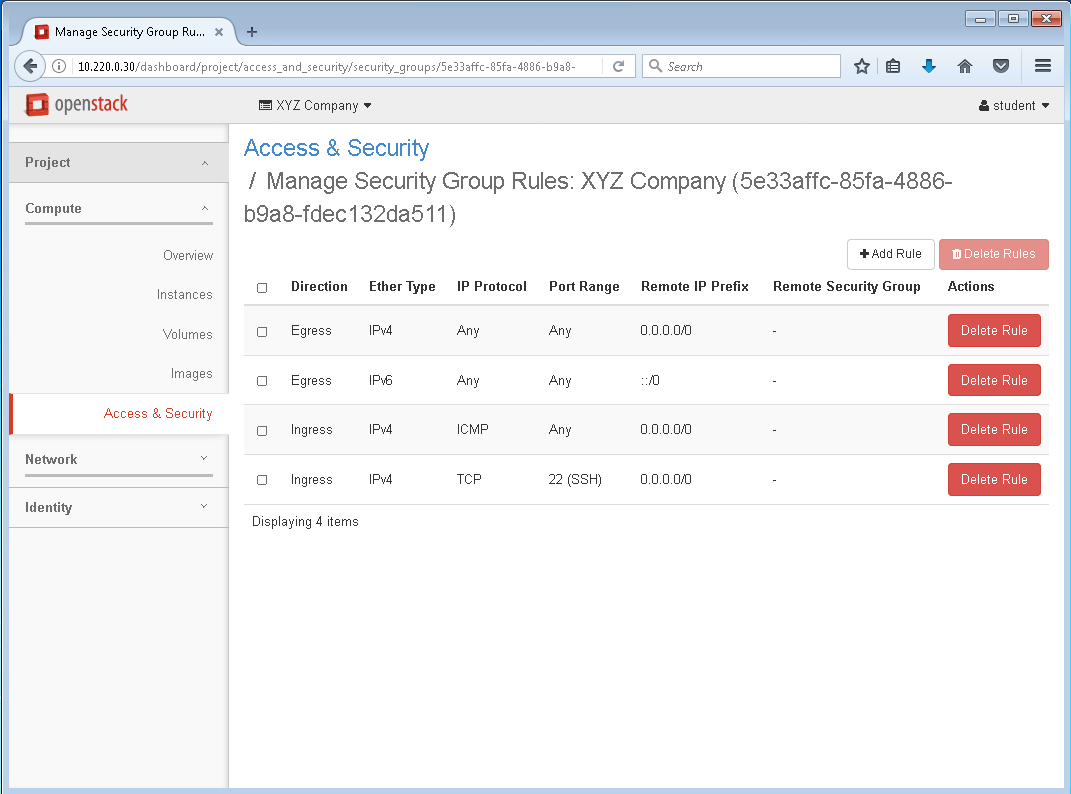
The CIDR block allows the user to designate a particular subnet or a specific IP Address as the only source that the Security Group would allow inbound network traffic from. For example: The OpenStack project manager could use their own desktop’s IP as the only source for inbound SSH traffic, but still allow http (web server) traffic from any address 0.0.0.0/0, which may enhance security.



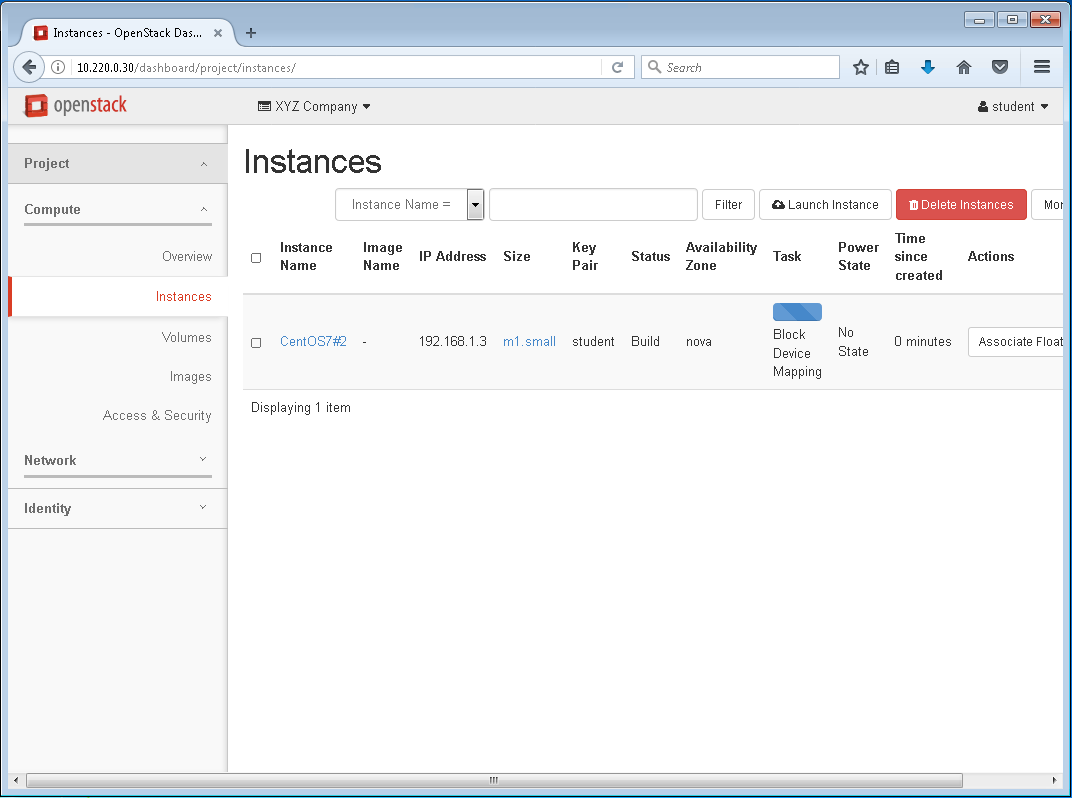
1. Scroll down, if necessary, and **Click** on **SSH**



1. Leave the Remote and CIDR at the defaults. **Click** on **Add**. **Repeat the previous steps** to add the **All ICMP** rule, with the **Direction, Remote, and CIDR at their defaults**, so that you can verify network connectivity using the ping command, if necessary

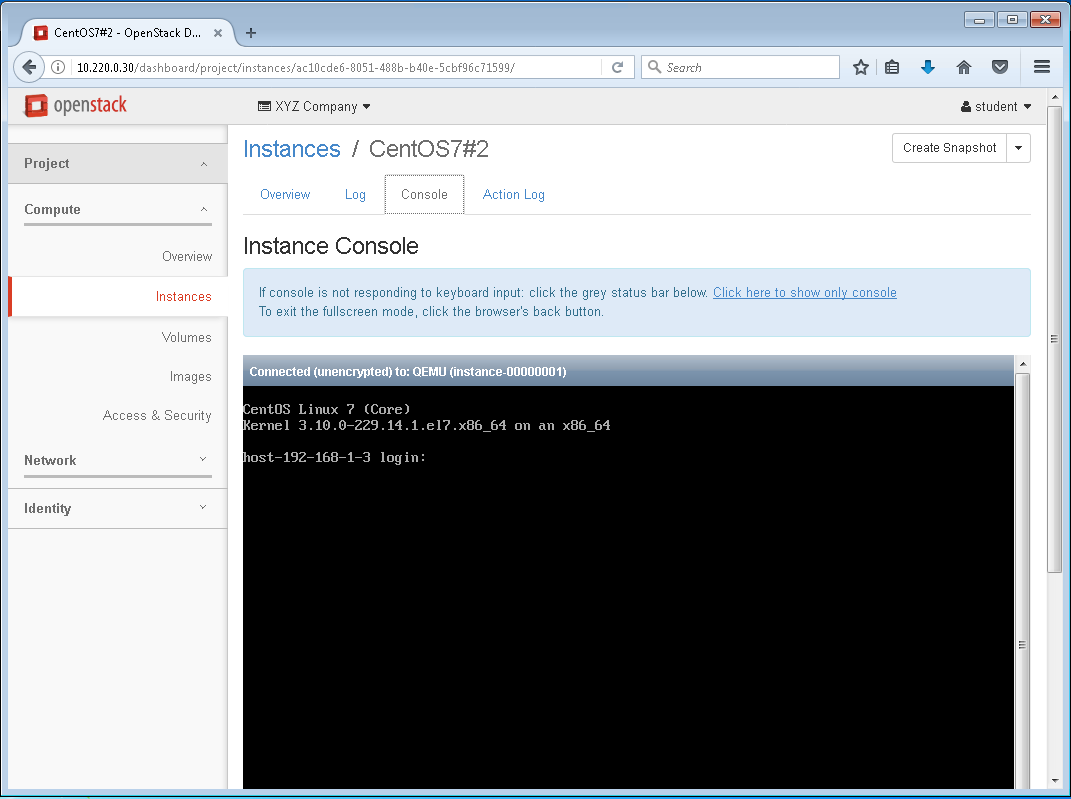


1. When completed, the XYZ Company Security Group rules should match this.



1. Launch an instance using the techniques presented in Module 4 using the information in the table below. Refer to Module 4 instructions, if necessary.

|  |  |
| --- | --- |
| Instance Name | CentOS7#2 |
| Source | CentOS |
| Flavor | m1.small |
| Network | private |
| Security Groups | XYZ Company |
| Key Pair | student |

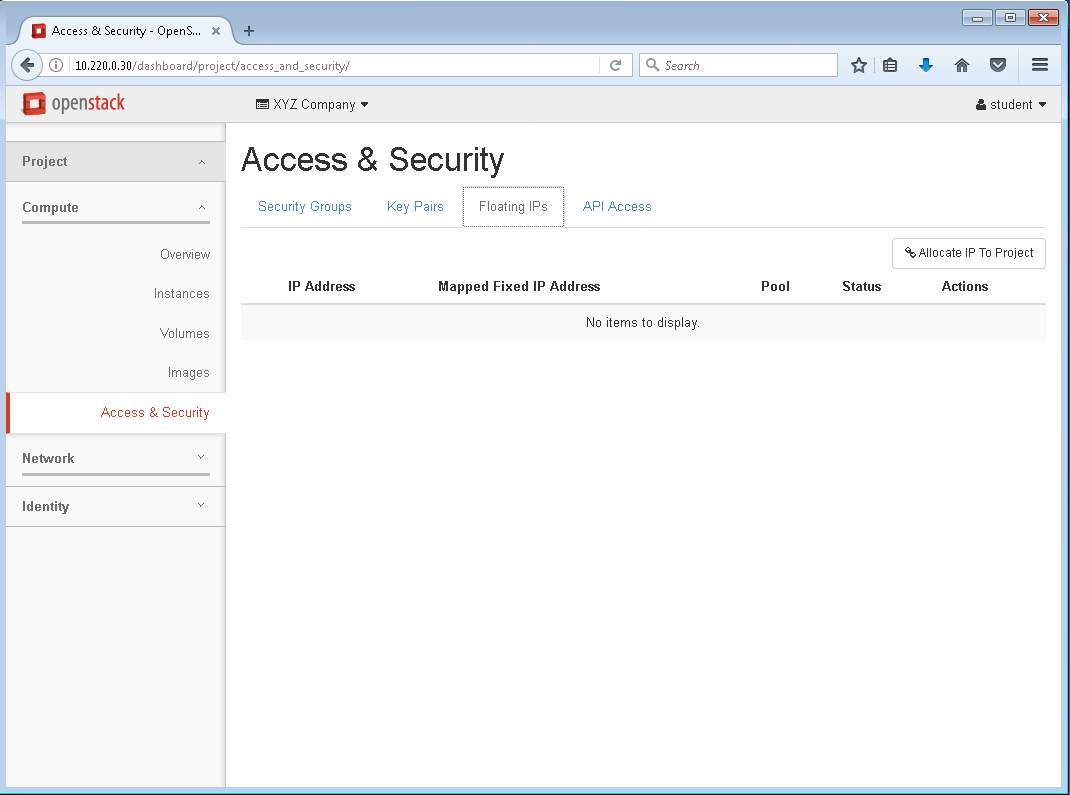


1. The CentOS7#2 instance should transition to the running state as shown in the screen capture above.

Note: Ensure that the CentOS7#2 instance is active and running before associating a Floating IP Address to it, this may take a couple minutes to complete.

Continue to Lab 13

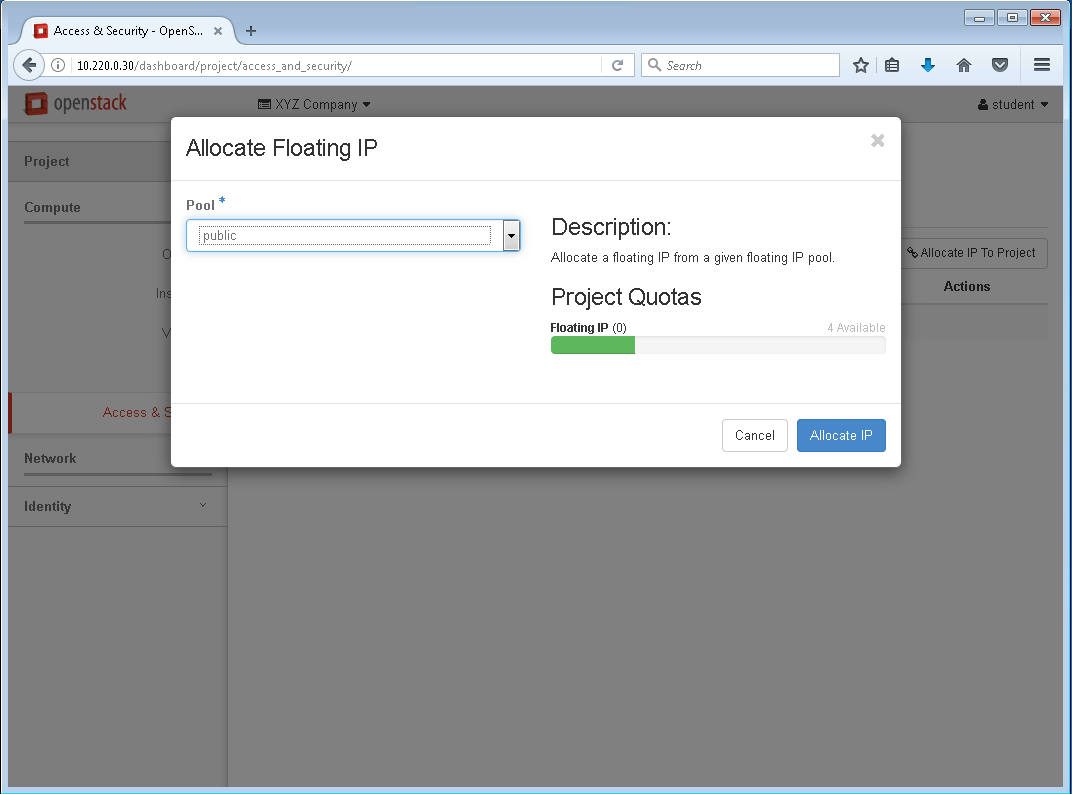
**Lab 13: Allocate and Associate a Floating IP Address to an OpenStack CentOS 7 Instance.**



1. Return to the Access & Security pane and the Floating IPs tab. **Click** on **Allocate IP to Project**

Instances tab

When the project is populated with an instance, or instances, the instance tab provides the user with a convenient location to quickly see particulars, for example: IP Addresses (internal and external), key-pairs and the current state of the virtual machine. Additionally, the dropdown menu provides additional options for configuring the instance.



1. The public network should be the default setting under the Pool, **Click Allocate IP**

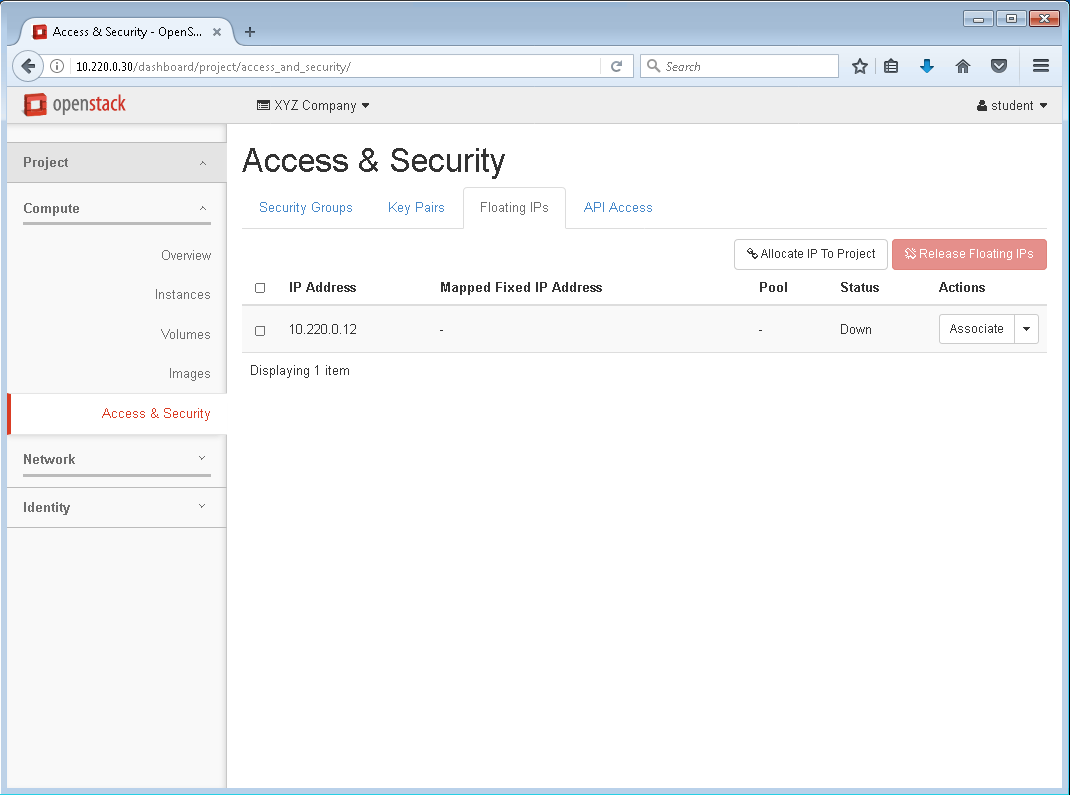
Routable IP Addresses

Non-routable (internal/private) IP address ranges are specifically reserved as follows:

10.0.0.0/8 172.16.0.0/12 192.168.0.0/16

Routable (external/public) IP address range is made up from the IP addresses not included above

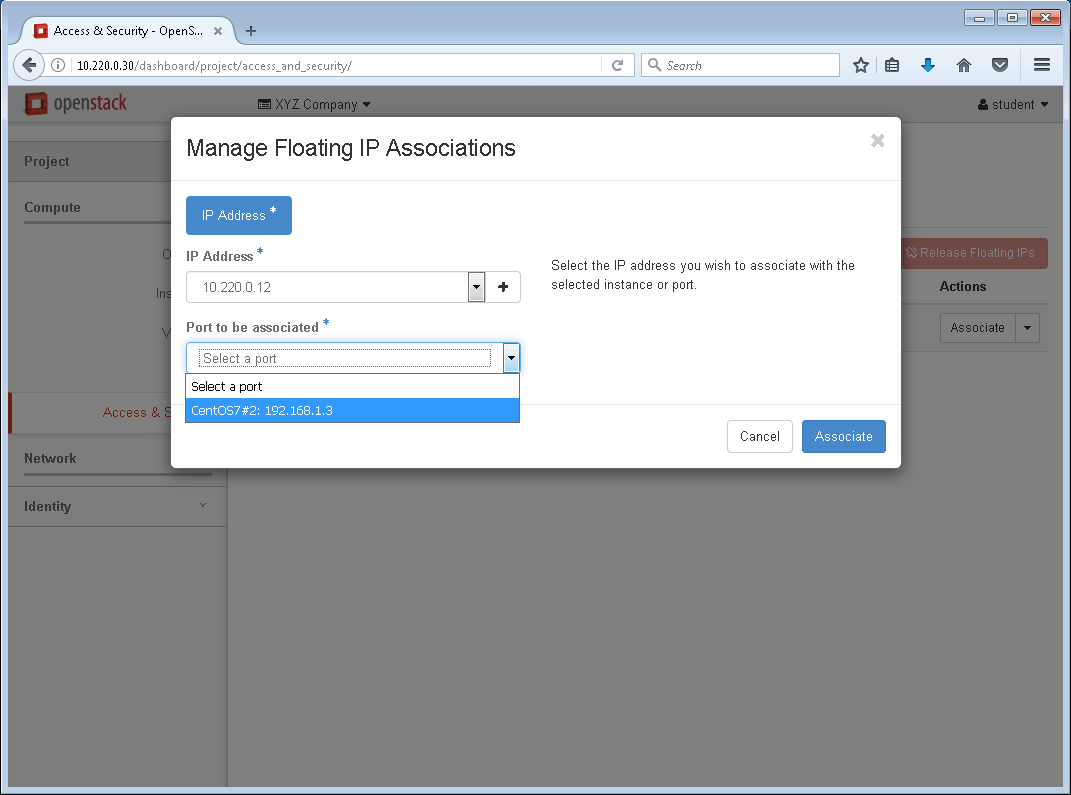
In the OpenStack environment, a pool of routable IP addresses are provided to the end user from the cloud provider, in this case the fictitious company CLOUDTech



1. The newly allocated IP address, 10.220.0.12, should appear, **Click** on Associate

Floating IP addresses

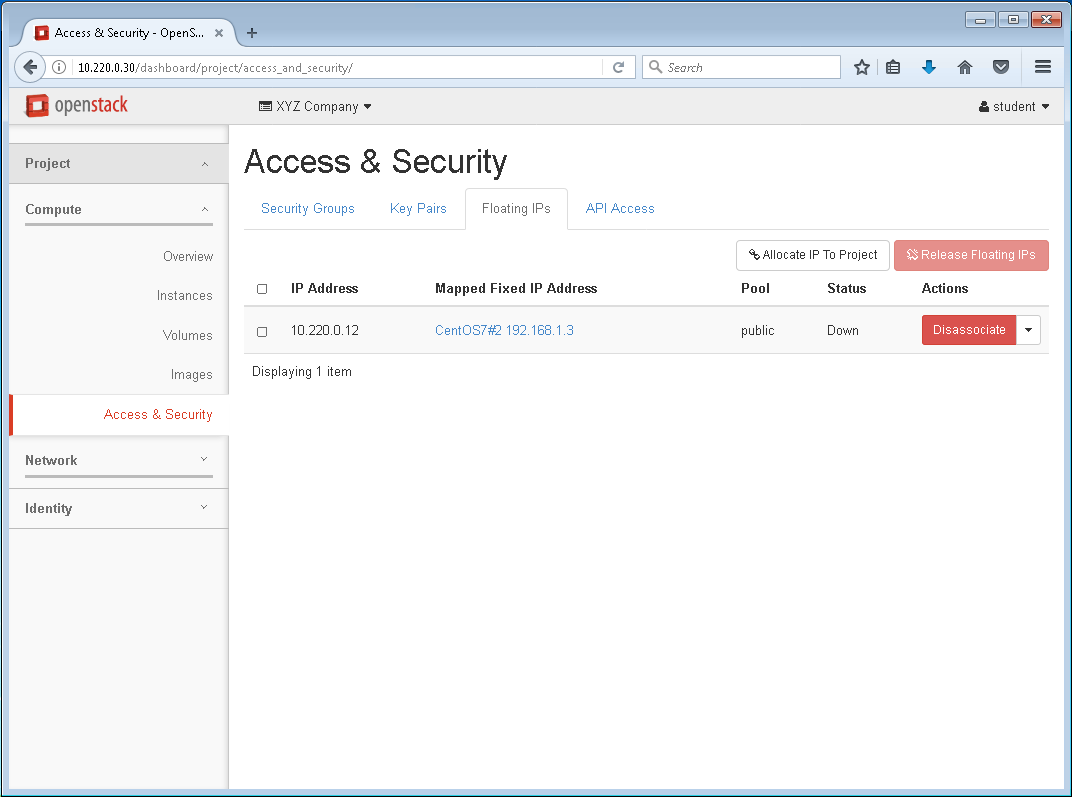
The floating IP address is associated by the end user to a particular instance, but can be released and associated to another instance.



1. From the Port to be associated drop down menu, **select CentOS#2: 192.168.1.3** and **Click** on **Associate**

Floating IP address pool

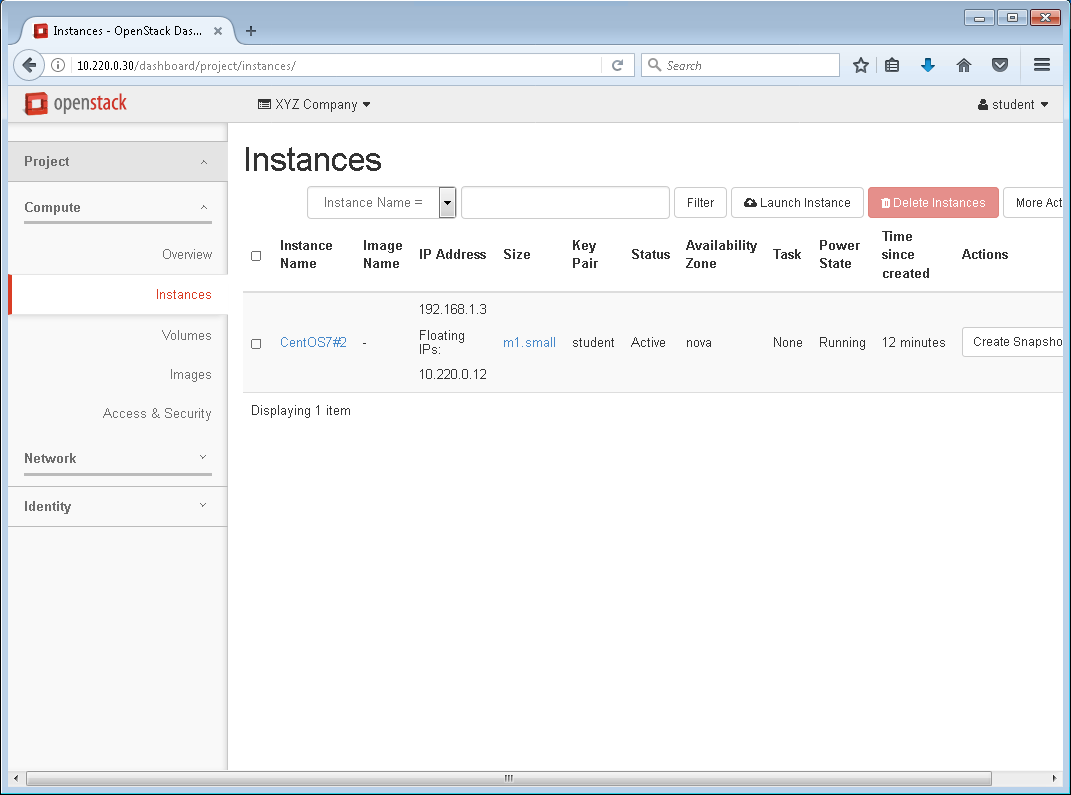
The cloud provider allocates a pool of floating IP addresses to a project, which gives the end user the option of associating a given IP address to an instance.

****

1. **CentOS7#2 192.168.1.3** should populate under the Mapped Fixed IP Address, **Click** on **the Instances tab**

Network Address Translation (NAT)

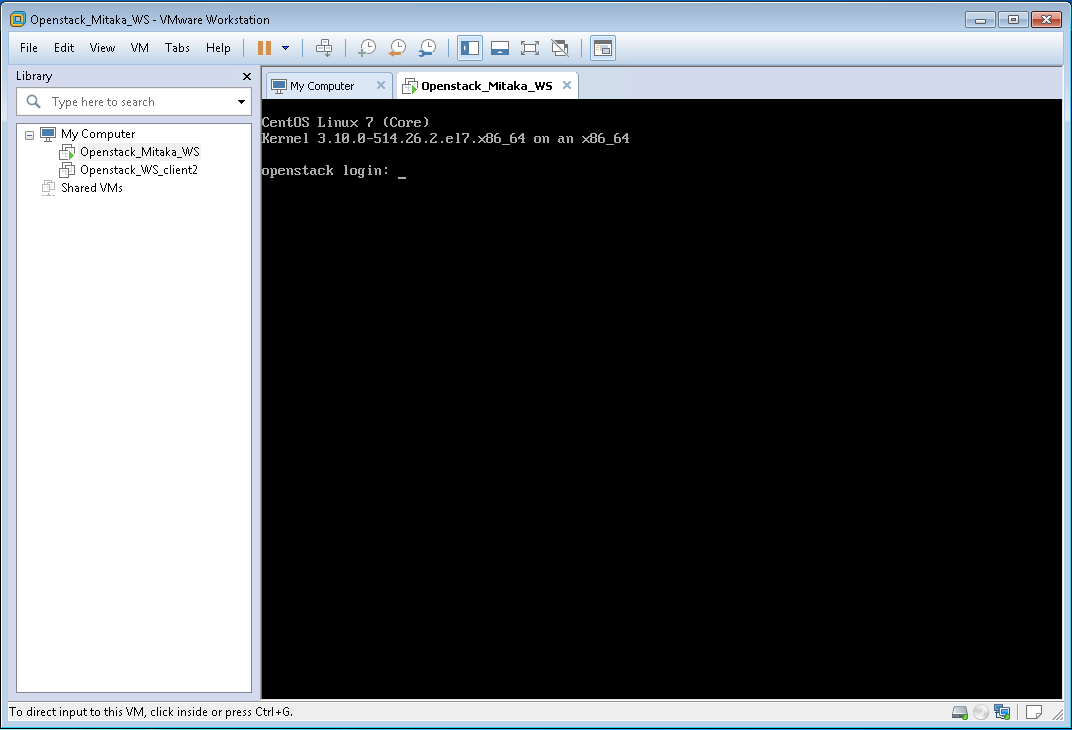
NAT is a process for modifying the source and destination addresses in the headers of an IP packet while the packet is in transit. This process enables network packets to move from the private IP address to the public IP address, without the receiver and sender applications being aware of the change.



1. Both IP Address, private and public, should be assigned to the CentOS7#2 instance

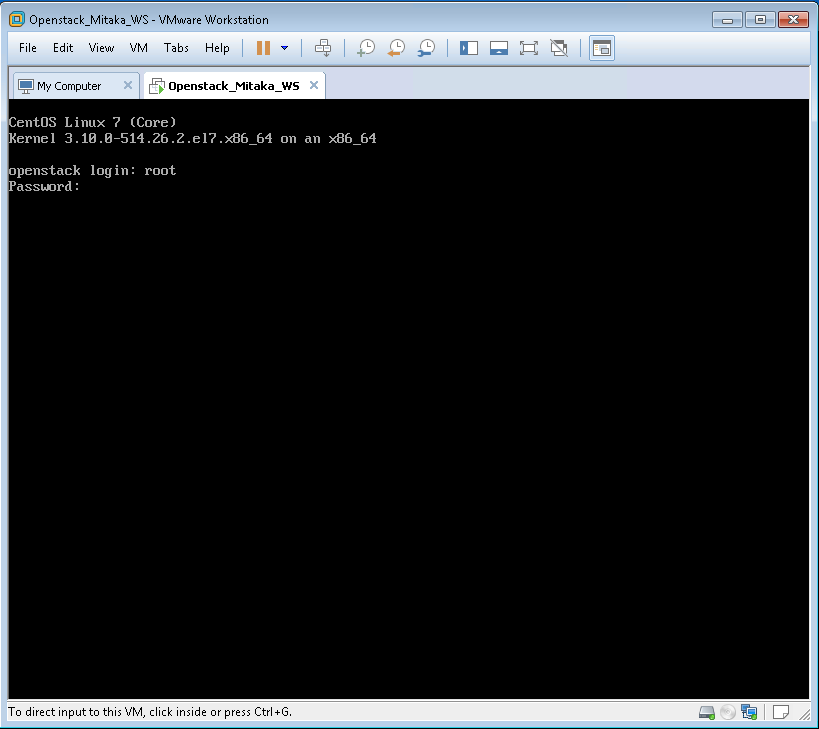
Continue to Grade Script

**Run the grade script**



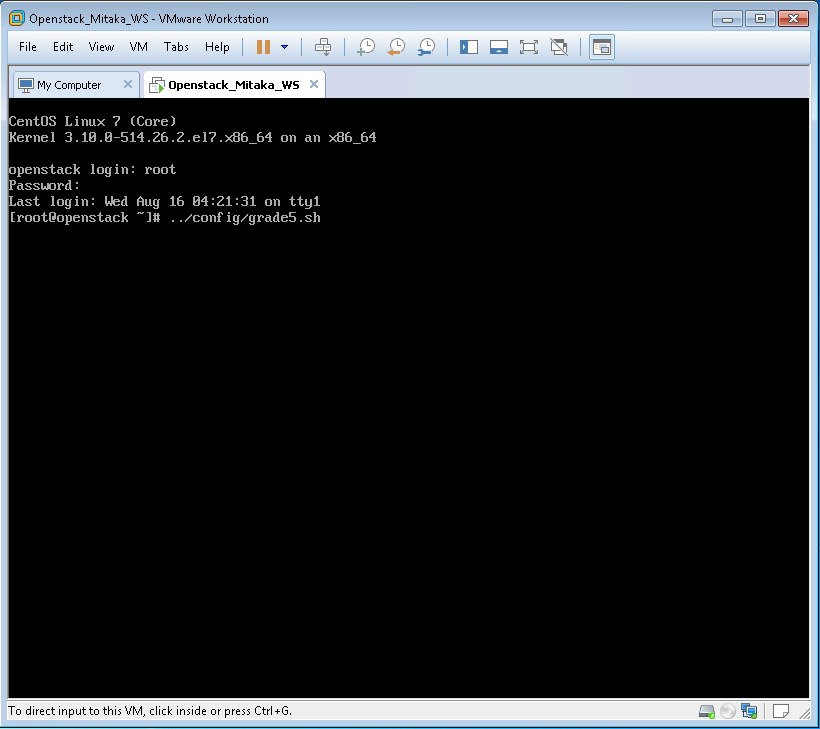
1. Return to Workstation and **Click** on **OpenStack\_Mitaka\_WS VM**

Note: The OpenStack\_Mitaka\_WS console may still be open on your desktop from when you ran the setup script

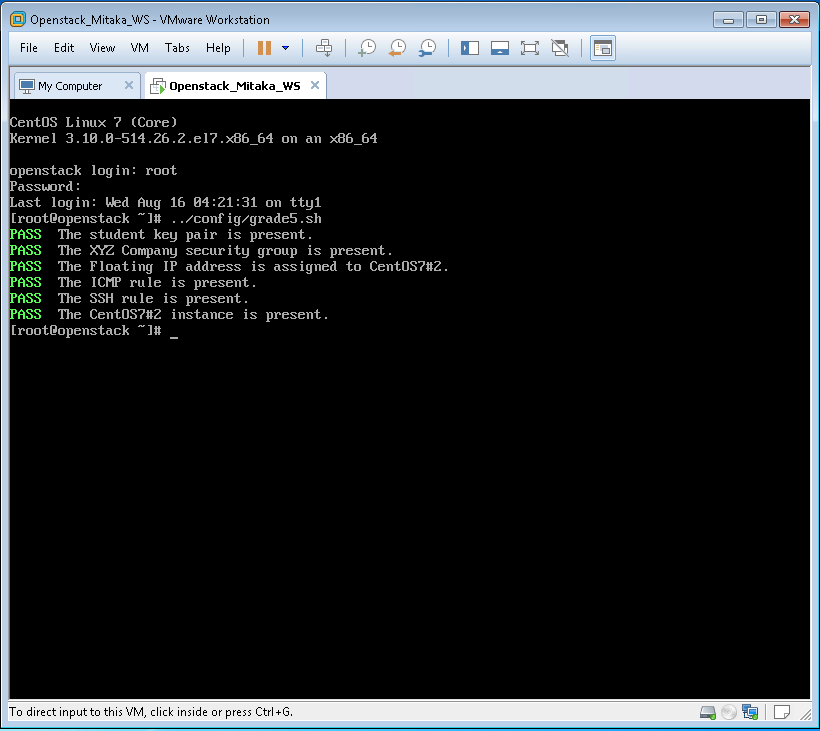


1. Log in as root with the Password: P@ssword

Note: The password is NOT visible as you type it



1. Enter the command; **../config/grade5.sh** and **press Enter**

****

1. 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\_v2 VM to the base snapshot and start over again.

This completes Module 5, continue to conclusion

**Conclusion:**

You have successfully assisted the customer in uploading a key pair, creating a security group and rules to allow both SSH and ICMP protocol traffic to the instance and associating a public IP address to an instance. Your next field visit to XYZ Company will be to show the user how to manage their key-pair and SSH into their CentOS 7 instance using PuTTY from a Windows VM and the Linux command line.