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.

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

Attributions:

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

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

Contents

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:

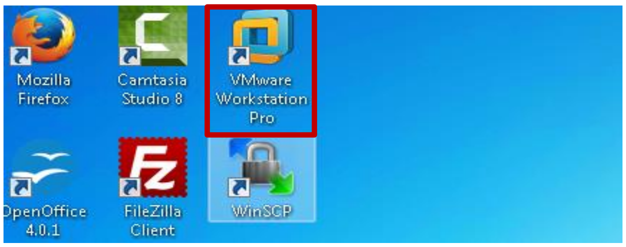
- Import a public key pair into OpenStack, Create a Security Group and Rules, and allocate a floating IP address to an instance.

Labs 11-13

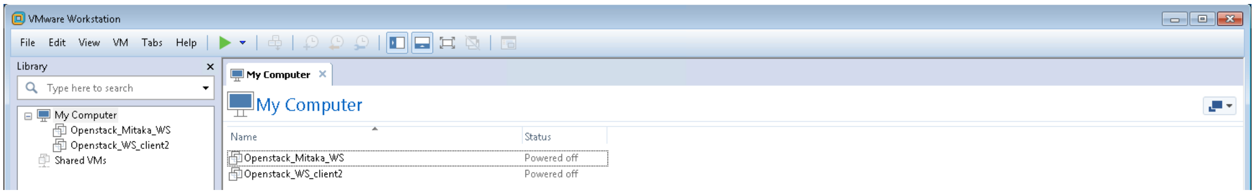
This lab will guide the student through importing a public key pair, creating a Security Group and Rules, and add a Floating IP address to an OpenStack project using the OpenStack Dashboard.

(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).

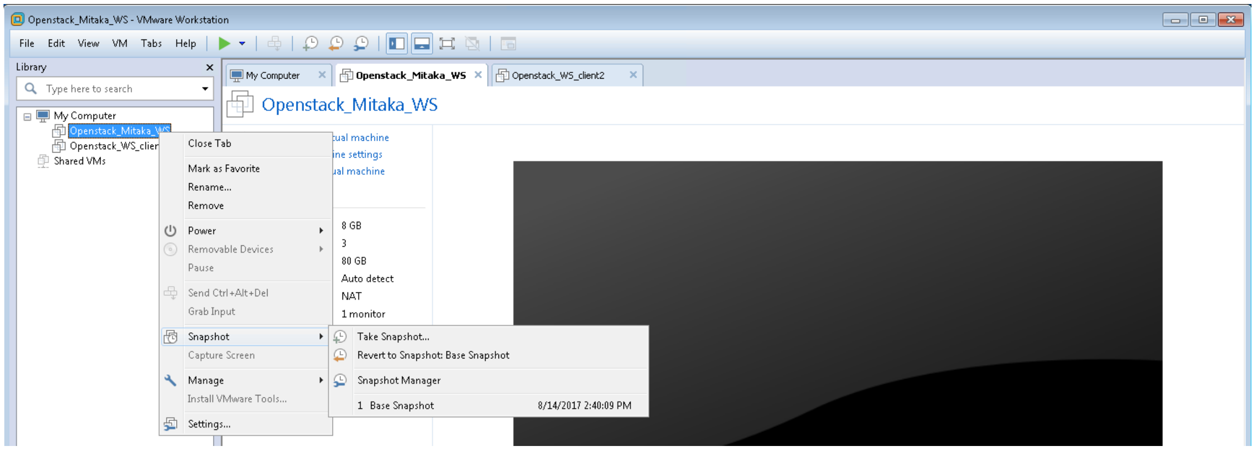
Prepare the OpenStack Virtual Machines



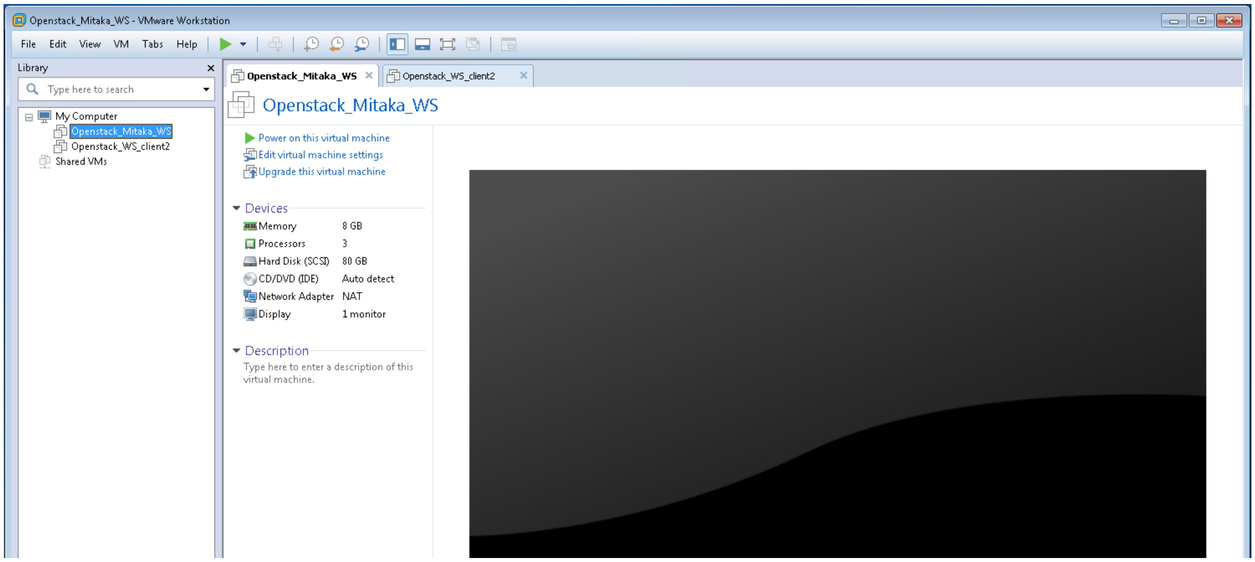
1. **Launch** the **VMware Workstation Pro application**



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.



Memory	8 GB
Processors	3
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Display	1 monitor

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 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.

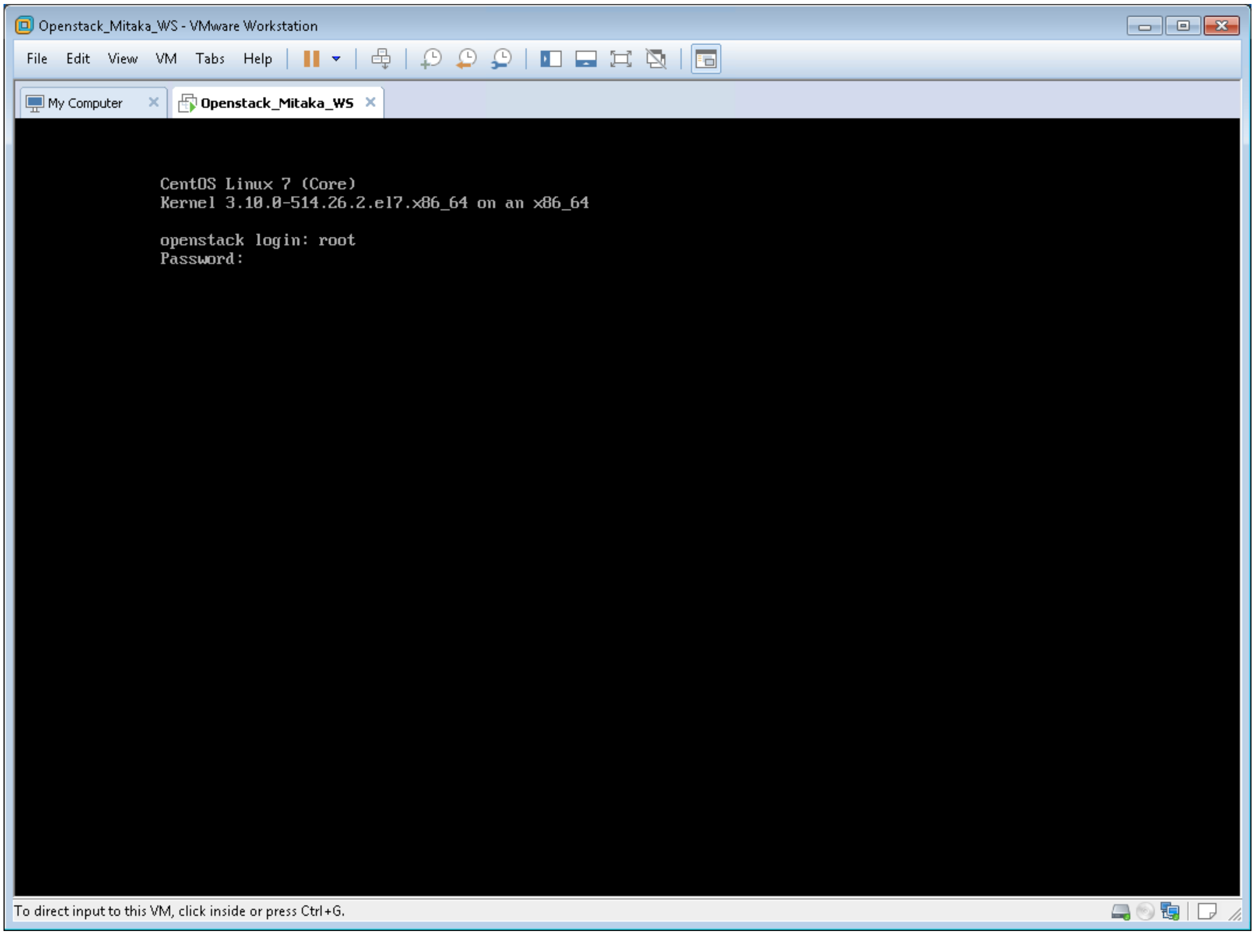
Lab Settings

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.

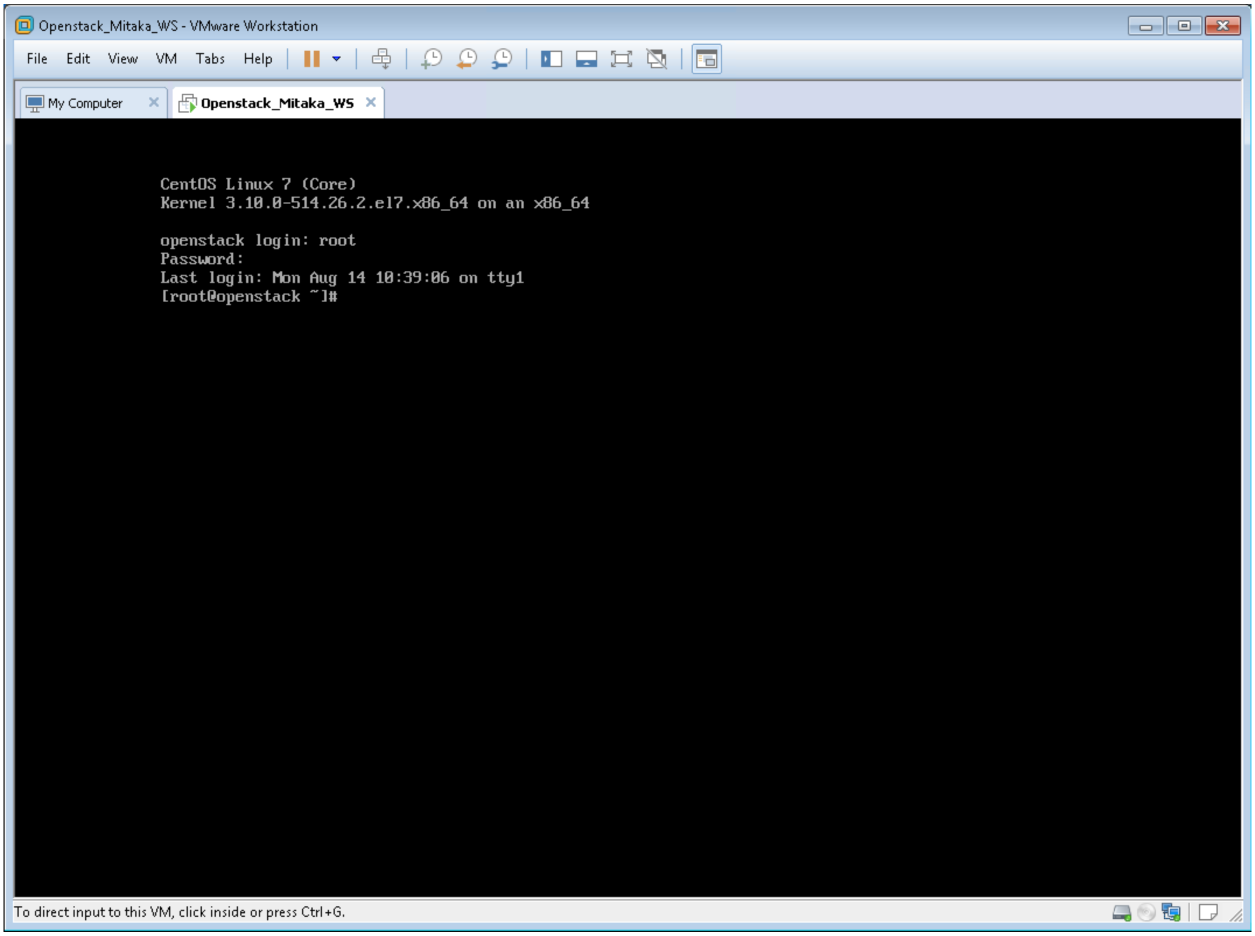
Run the lab setup script


Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
My Computer
Openstack_Mitaka_WS
To direct input to this VM, click inside or press Ctrl+G.

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

openstack login: root
Password:
```

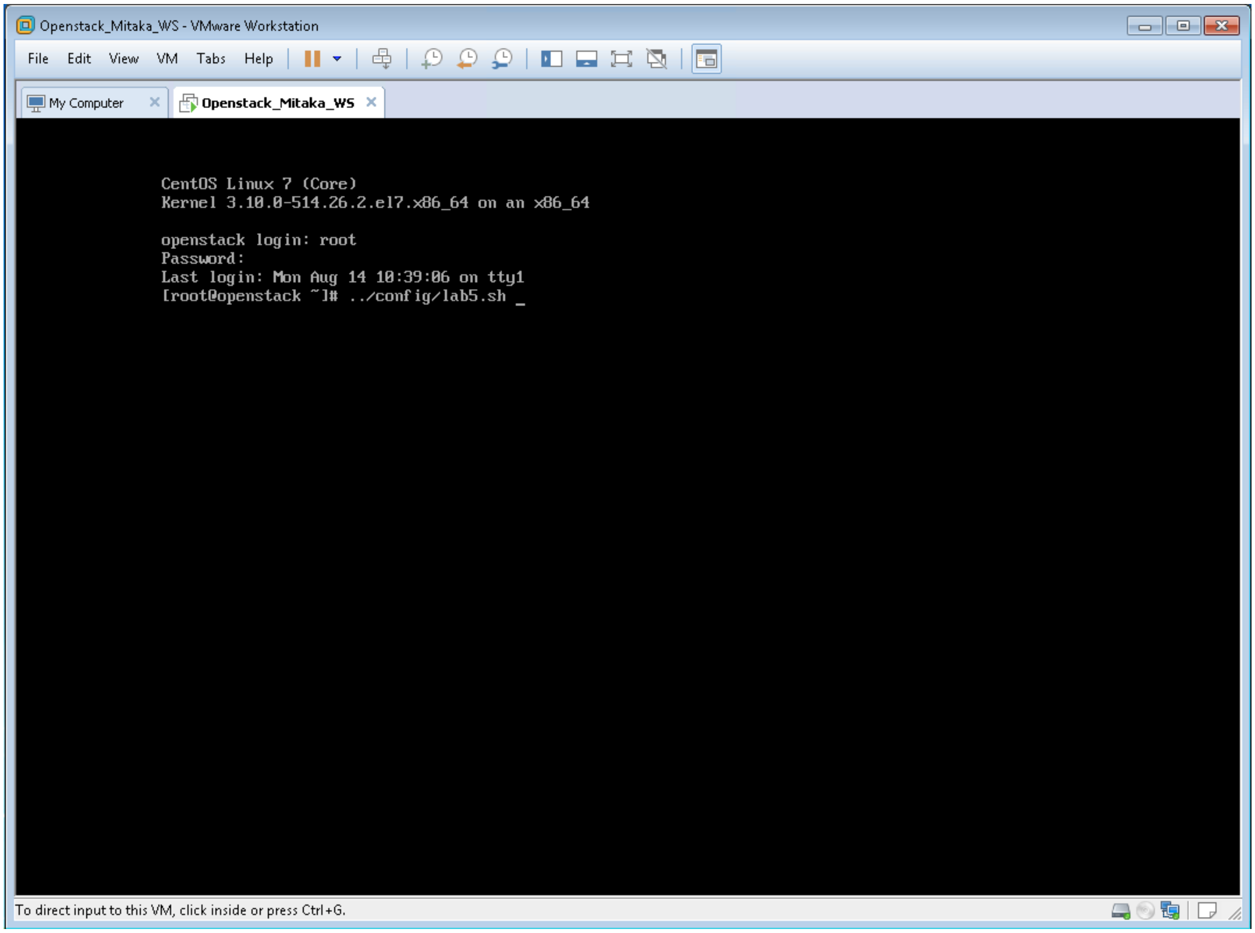
1. Log in as **root** with the Password: **P@ssword**

   Note: The password is NOT visible as you type it


Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
My Computer
Openstack_Mitaka_WS
To direct input to this VM, click inside or press Ctrl+G.

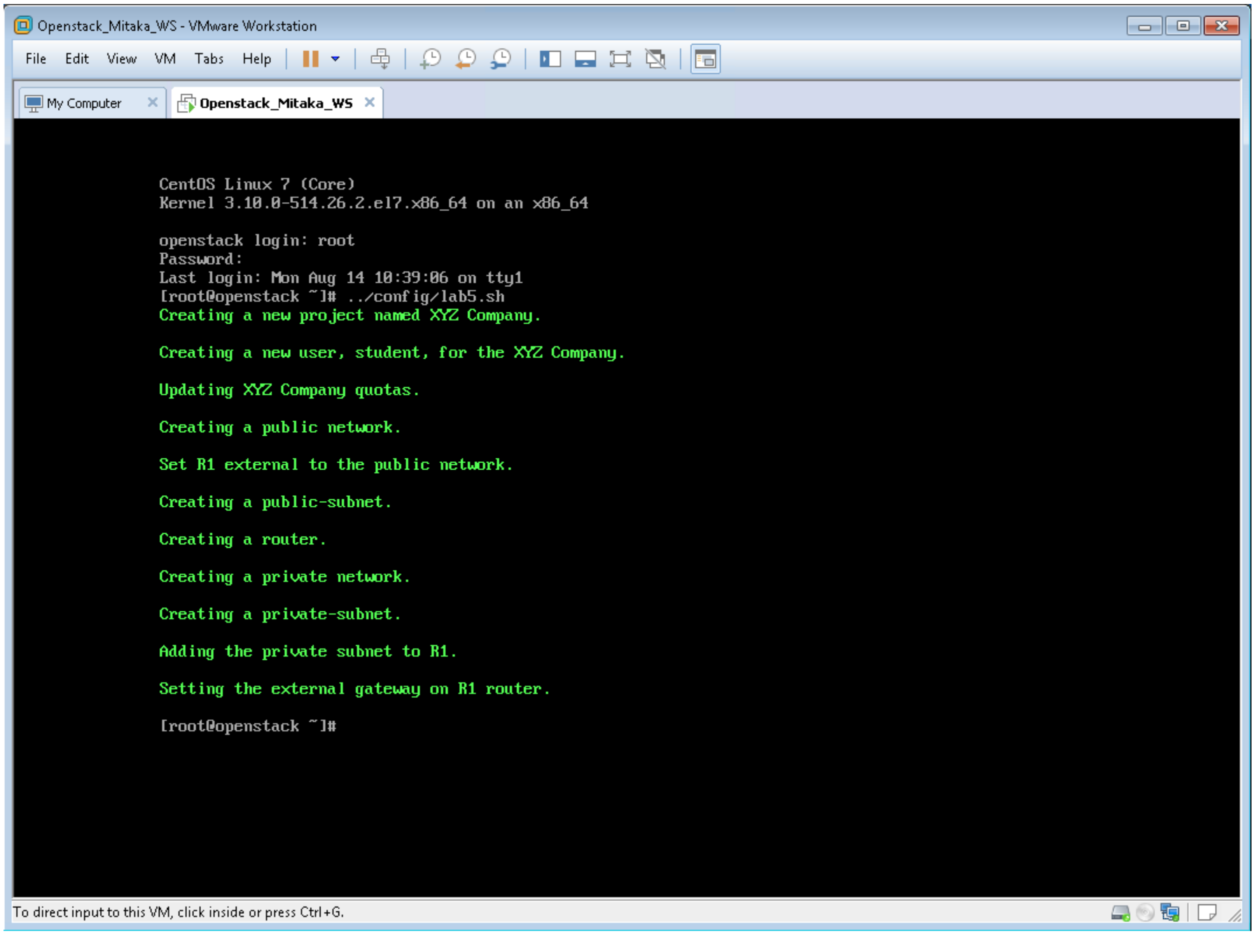
```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.2.el7.x86_64 on an x86_64

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

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


Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
My Computer
Openstack_Mitaka_WS
To direct input to this VM, click inside or press Ctrl+G.

```
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/lab5.sh _
```

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

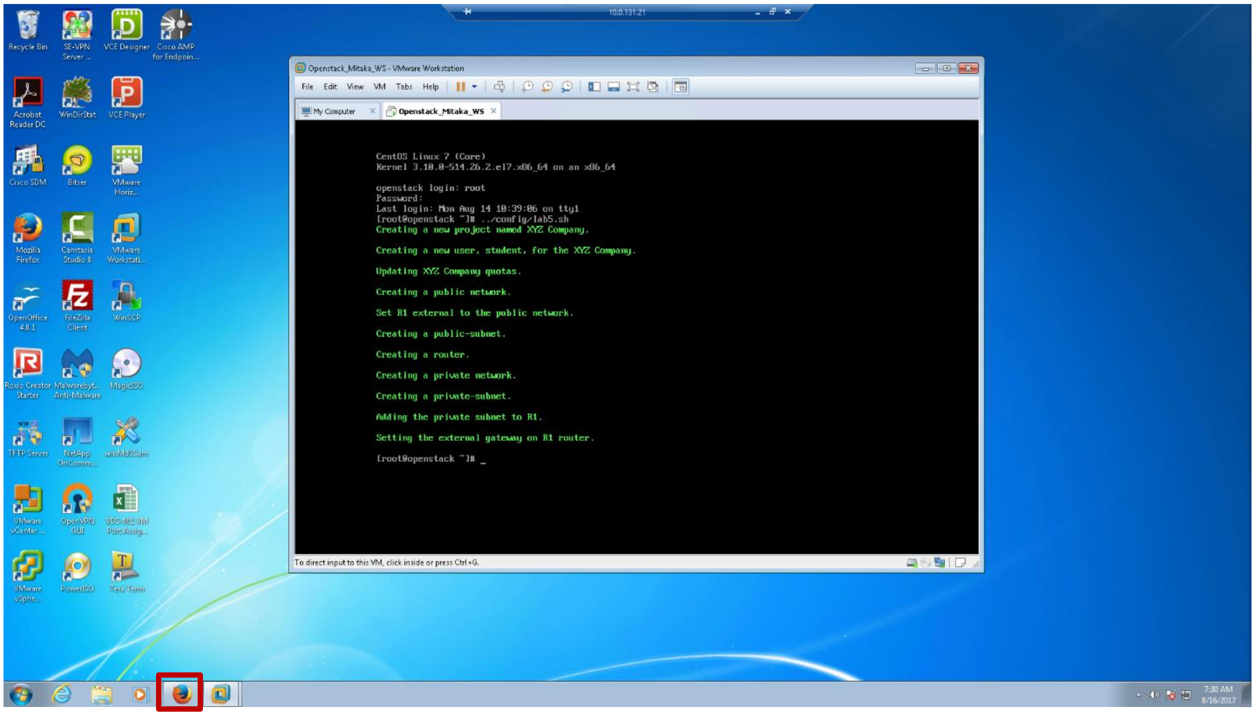

Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
My Computer
Openstack_Mitaka_WS
To direct input to this VM, click inside or press Ctrl+G.

```
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/lab5.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.

[root@openstack ~]#
```

4. 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

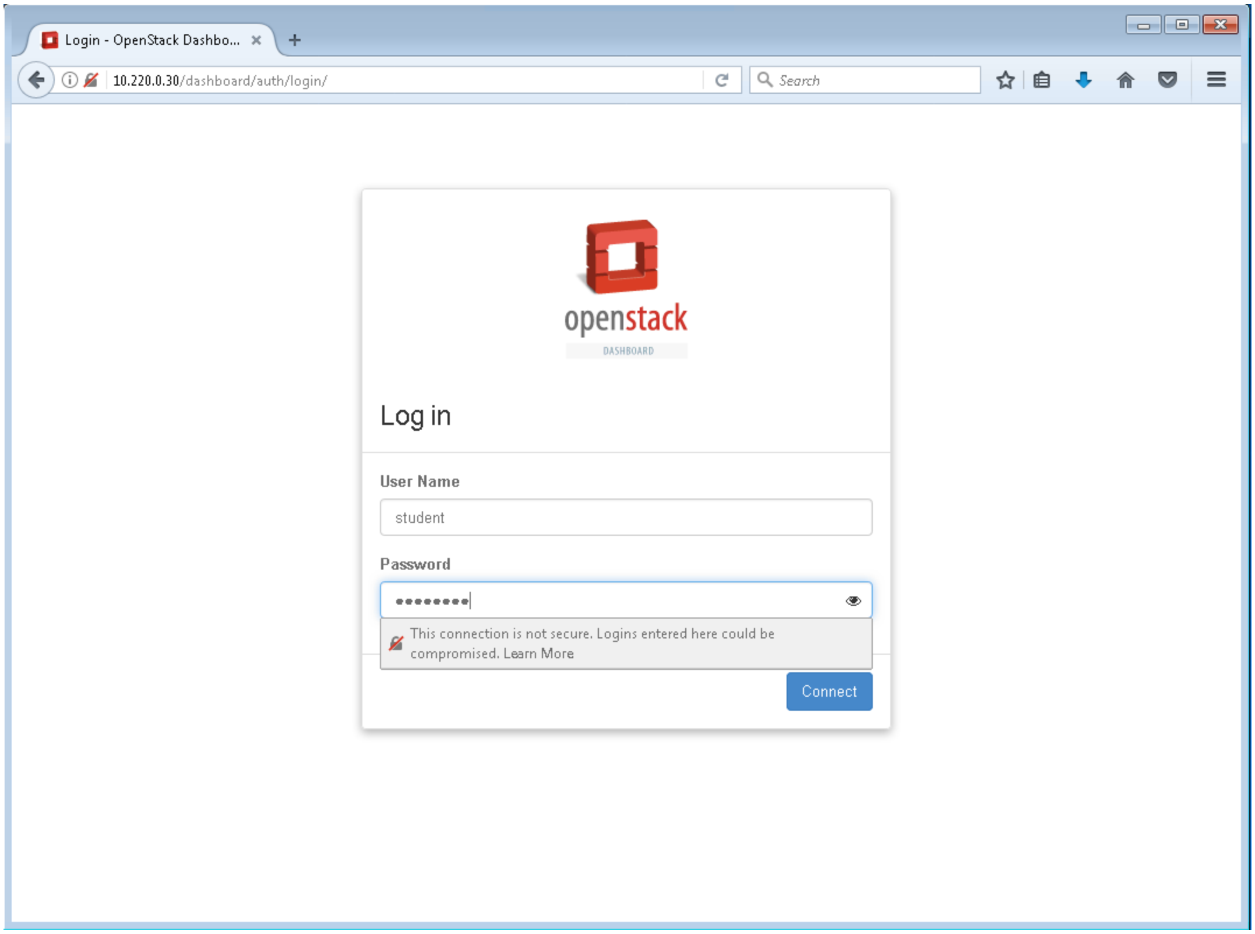

Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
My Computer
Openstack_Mitaka_WS

```
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/lab5.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.

[root@openstack ~]# _
```

To direct input to this VM, click inside or press Ctrl+G.

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.


Login - OpenStack Dashbo...
10.220.0.30/dashboard/auth/login/
Search
openstack
DASHBOARD

Log in

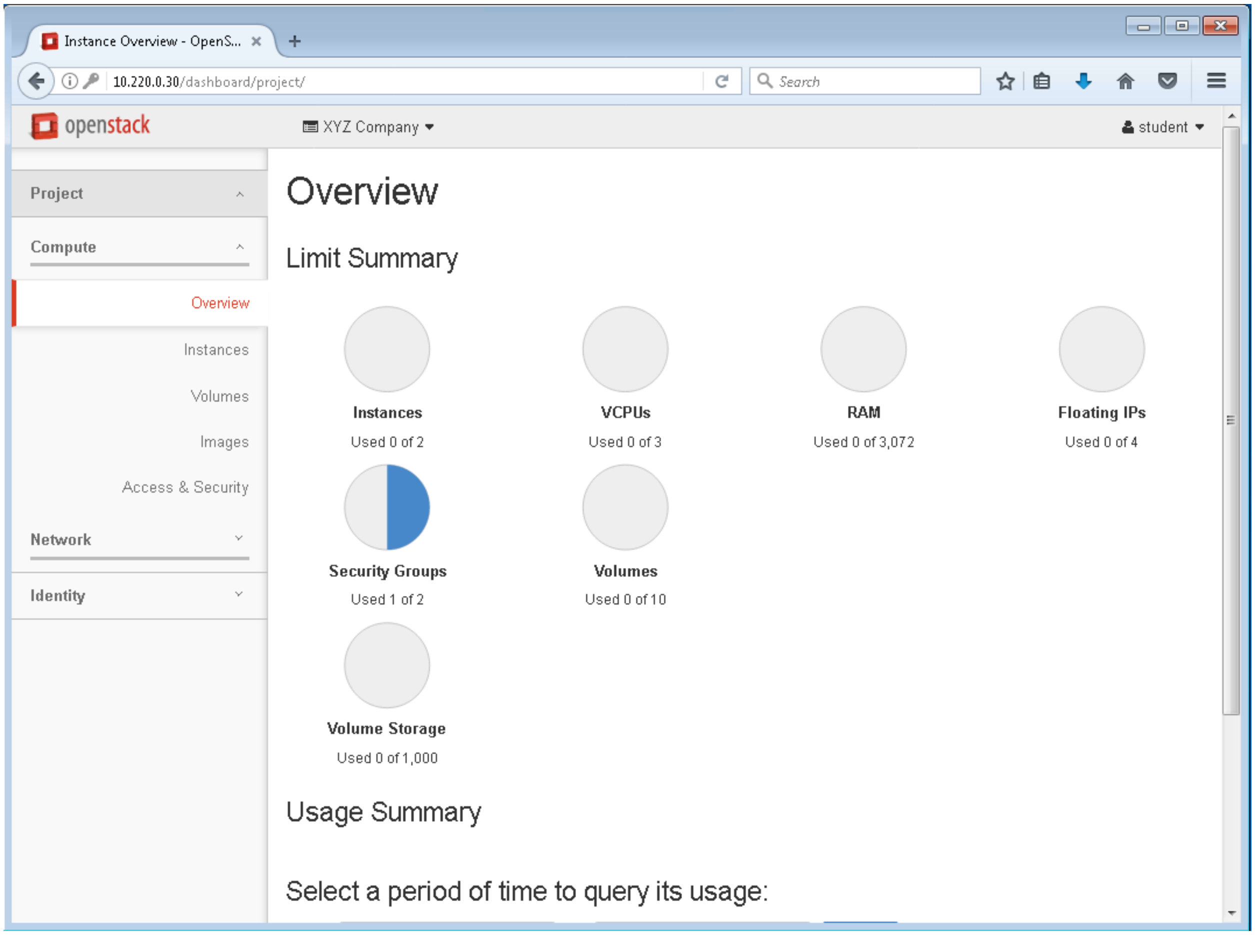
User Name: student

Password: ••••••••

This connection is not secure. Logins entered here could be compromised. Learn More

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.



Overview

Limit Summary

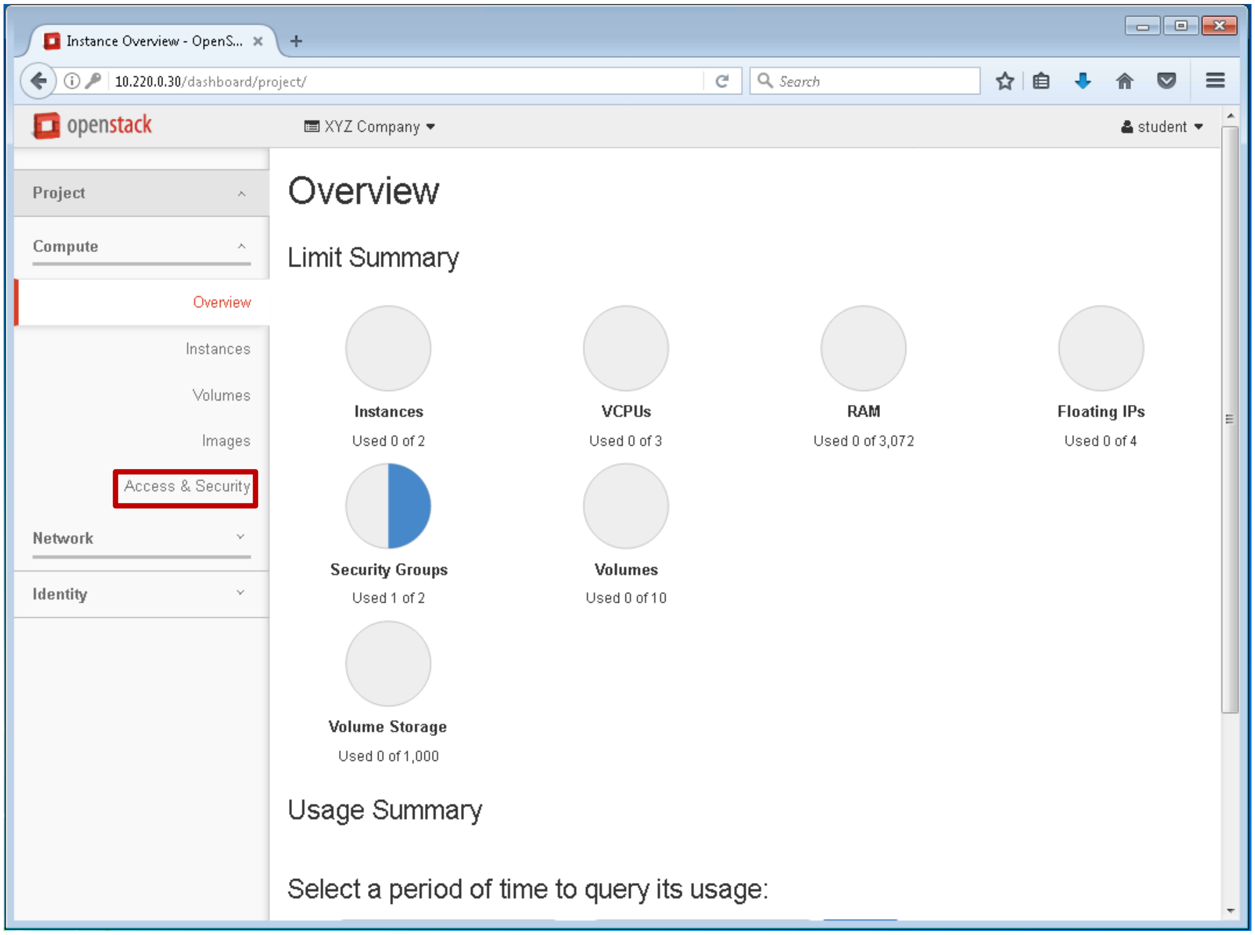
Instances	Used 0 of 2
VCPUs	Used 0 of 3
RAM	Used 0 of 3,072
Floating IPs	Used 0 of 4
Security Groups	Used 1 of 2
Volumes	Used 0 of 10
Volume Storage	Used 0 of 1,000

Usage Summary

Select a period of time to query its usage:

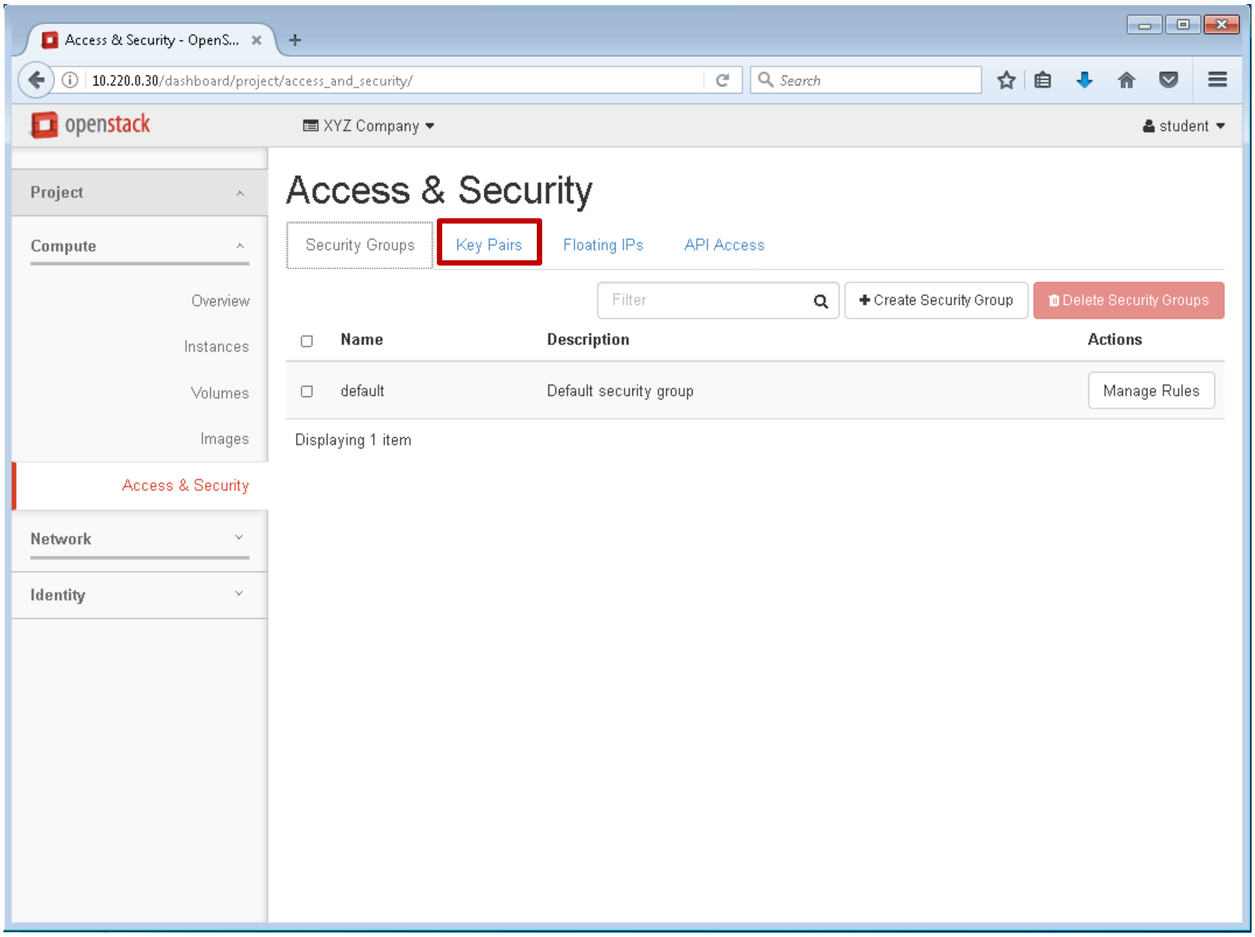
5. This is the homepage of the OpenStack Dashboard as seen from the XYZ Companies' customer perspective.

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.

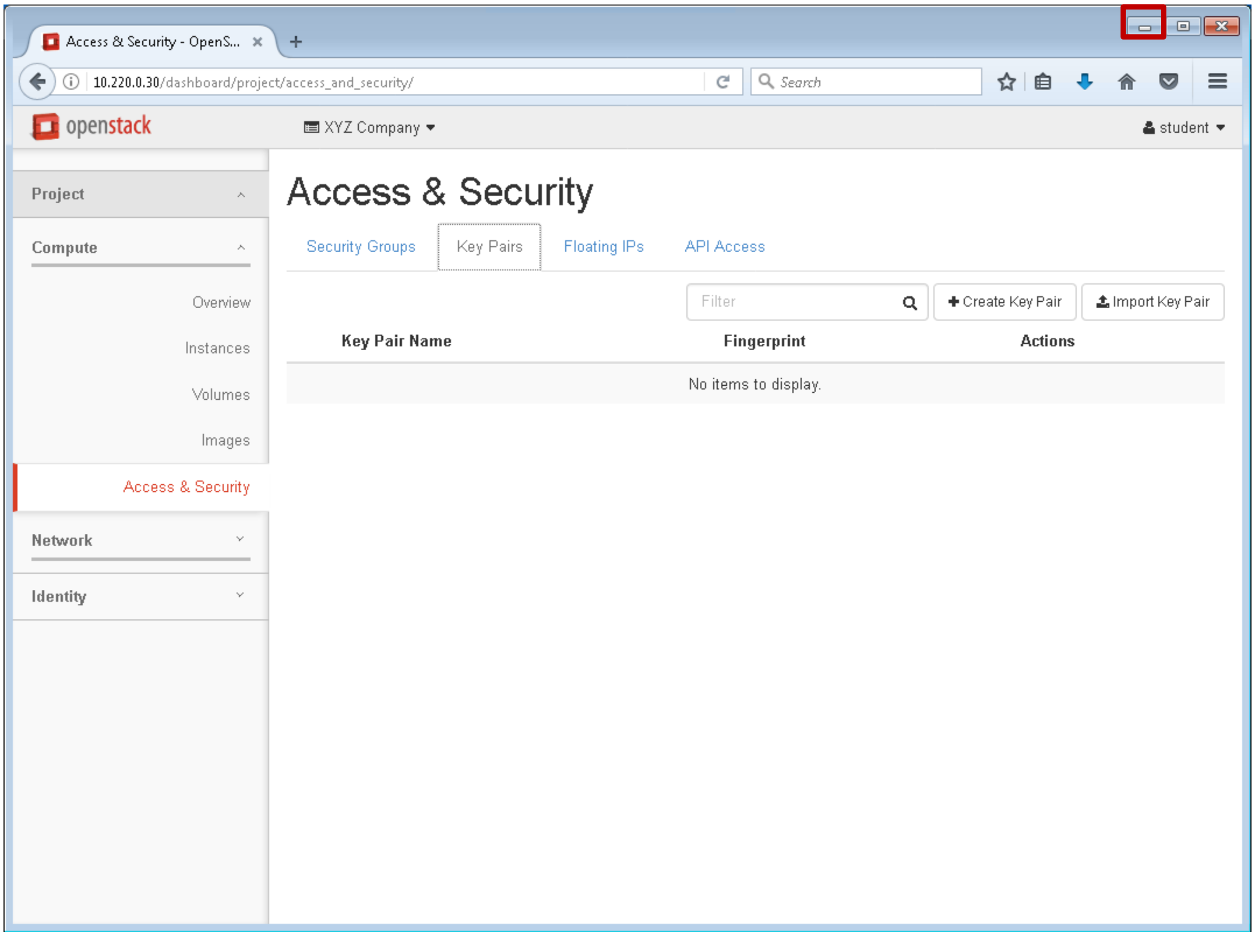


Access & Security

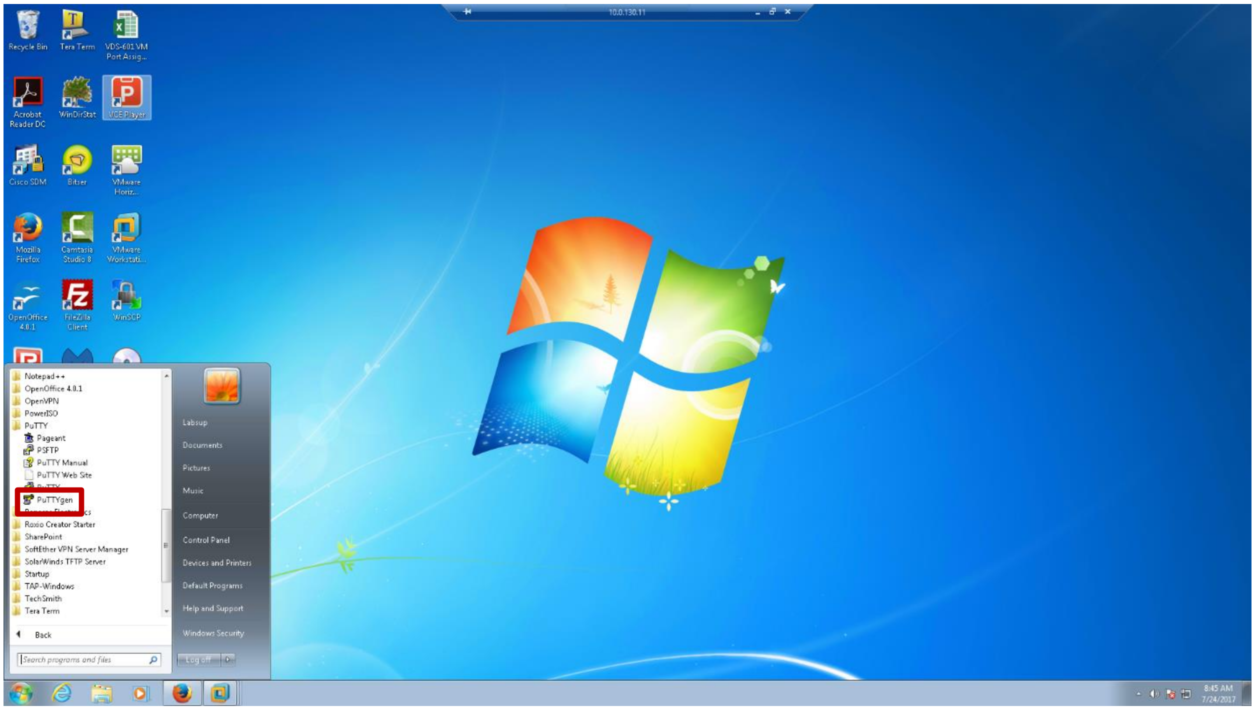
☐	Name	Description	Actions
☐	default	Default security group	Manage Rules

Displaying 1 item

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

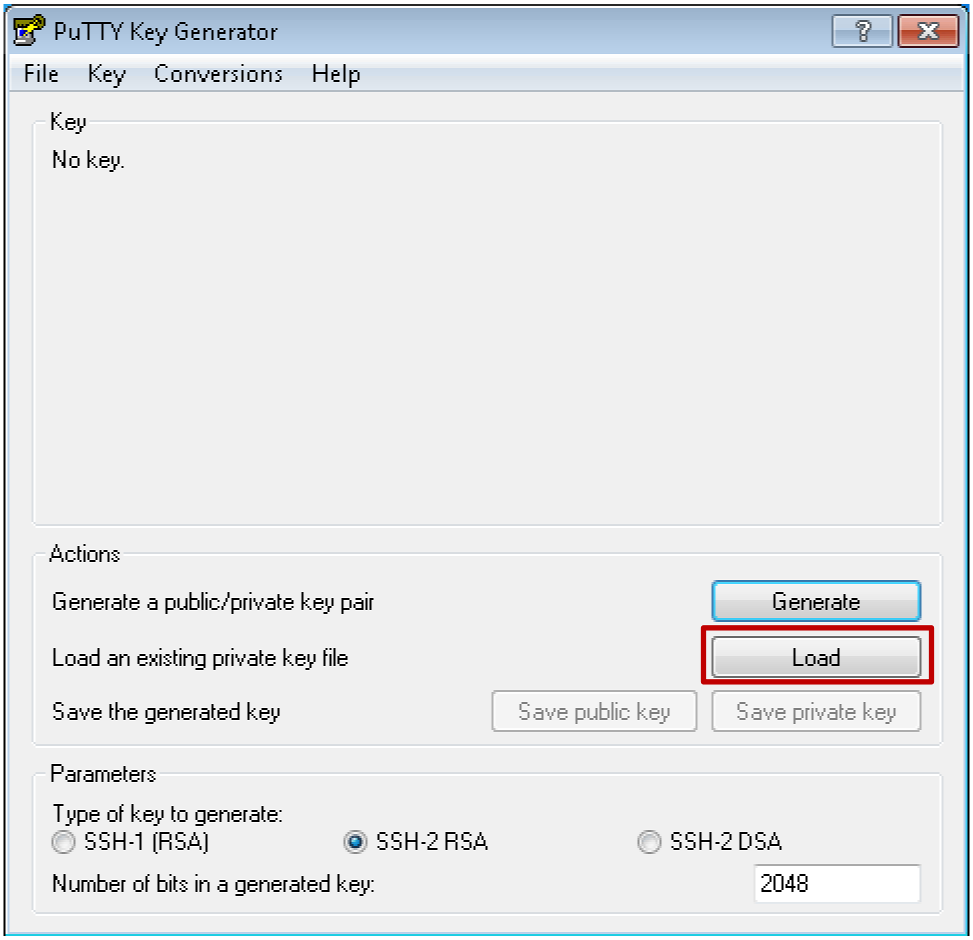


3. **Minimize** the **OpenStack web page**

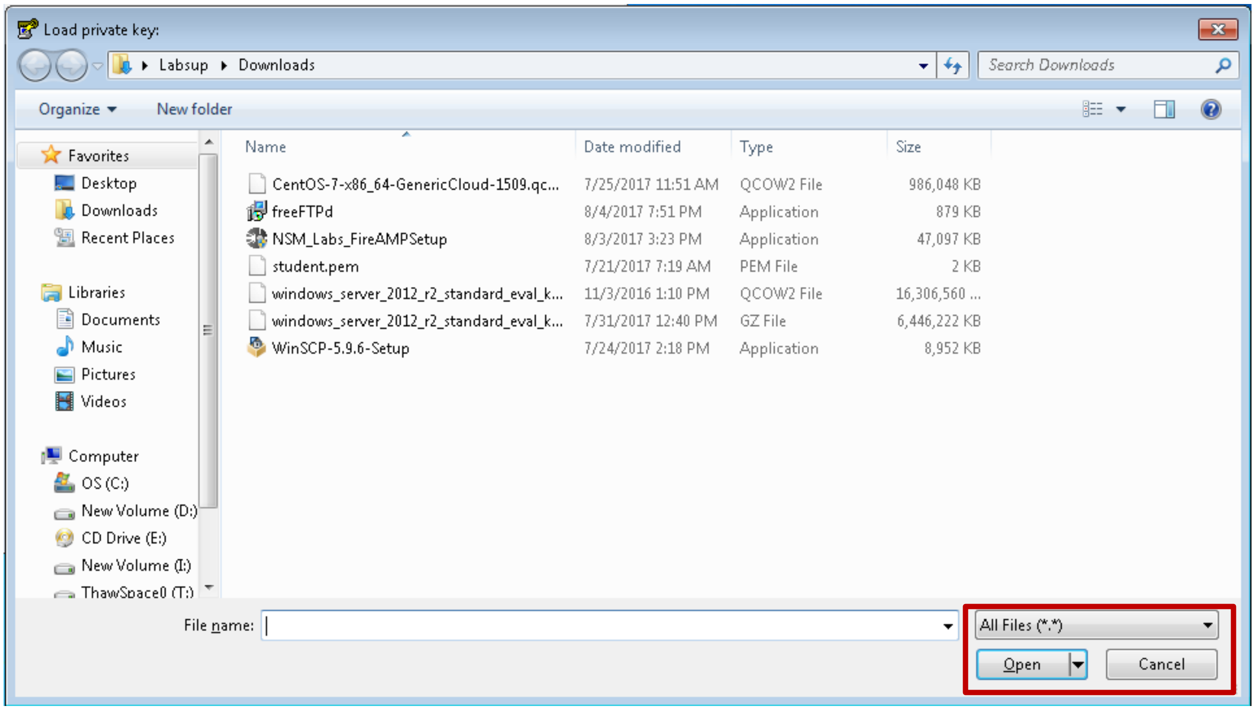


4. **Open PuTTY Key Generator** All Programs>PuTTY>PuTTYgen

   Note: Representative image, your host will be different.



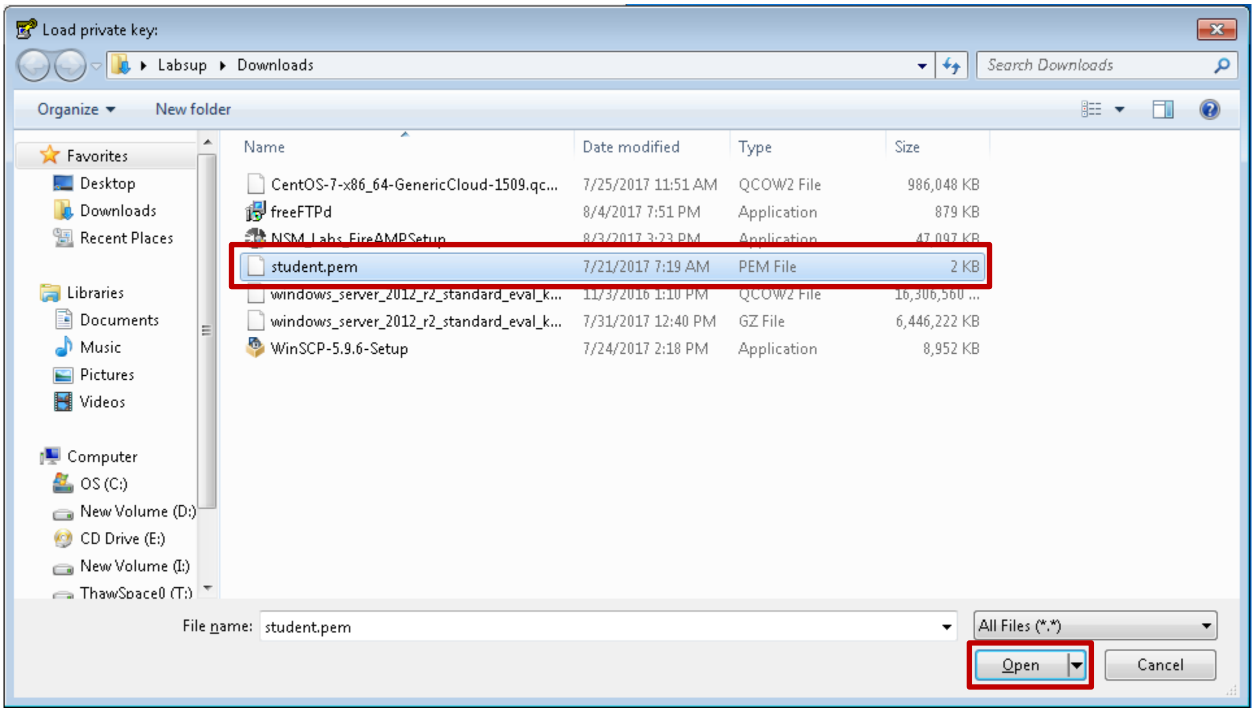
5. **Click** on **Load**



Name	Date modified	Type	Size
CentOS-7-x86_64-GenericCloud-1509.qc...	7/25/2017 11:51 AM	QCOW2 File	986,048 KB
freeFTPd	8/4/2017 7:51 PM	Application	879 KB
NSM_Labs_FireAMPSetup	8/3/2017 3:23 PM	Application	47,097 KB
student.pem	7/21/2017 7:19 AM	PEM File	2 KB
windows_server_2012_r2_standard_eval_k...	11/3/2016 1:10 PM	QCOW2 File	16,306,560 ...
windows_server_2012_r2_standard_eval_k...	7/31/2017 12:40 PM	GZ File	6,446,222 KB
WinSCP-5.9.6-Setup	7/24/2017 2:18 PM	Application	8,952 KB

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

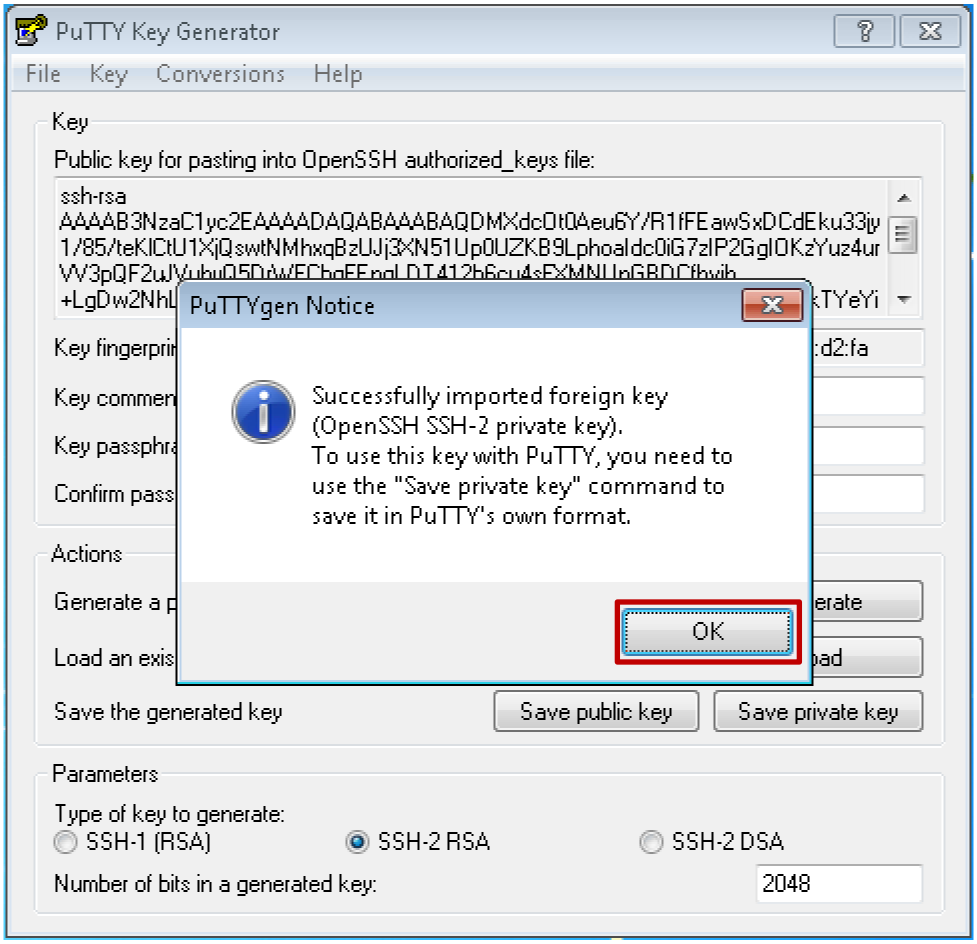
   Note: Representative image, your host downloads folder will not contain the same items.



Name	Date modified	Type	Size
CentOS-7-x86_64-GenericCloud-1509.qc...	7/25/2017 11:51 AM	QCOW2 File	986,048 KB
freeFTPd	8/4/2017 7:51 PM	Application	879 KB
NSM_Labs_FireAMPSetup	8/3/2017 3:23 PM	Application	47,097 KB
student.pem	7/21/2017 7:19 AM	PEM File	2 KB
windows_server_2012_r2_standard_eval_k...	11/3/2016 1:10 PM	QCOW2 File	16,306,560 ...
windows_server_2012_r2_standard_eval_k...	7/31/2017 12:40 PM	GZ File	6,446,222 KB
WinSCP-5.9.6-Setup	7/24/2017 2:18 PM	Application	8,952 KB

File name: student.pem

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



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDMXdc0t0Aeu6Y/R1fFEawSxDCdEku33jy
1/85/teKlCtU1XjQswtNMhxqBzUJj3XN51Up0UZKB9Lphoaldc0iG7zlP2GglOKzYuz4ur
```

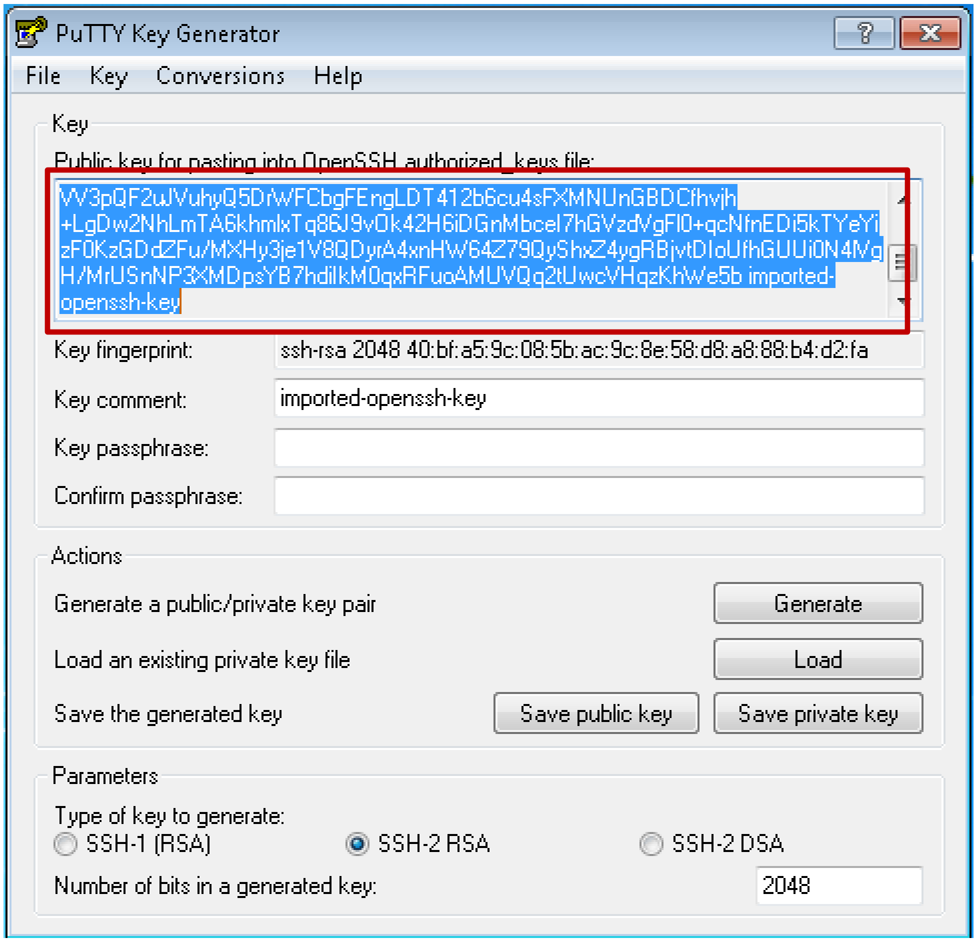
PuTTYgen Notice

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.

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

Number of bits in a generated key: 2048

8. **Click OK** to proceed



Public key for pasting into OpenSSH authorized_keys file:

```
VV3pQF2uJVuhyQ5DrWFCbgFEngLDT412b6cu4sFXMNUnGBDCfhvjh
+LgDw2NhLmTA6khmlxTq86J9v0k42H6iDGnMbcel7hGVzdVgFl0+qcNfnEDi5kTYeYi
zF0KzGDdZFu/MXHy3je1V8QDyrA4xnHW64Z79QyShxZ4ygRBjvtDIoUfhGUUi0N4Mg
H/MrUSnNP3XMDpsYB7hdilkM0qxRFuoAMUVQq2tUwcVHqzKhWe5b imported-
openssh-key
```

Key fingerprint: ssh-rsa 2048 40:bf:a5:9c:08:5b:ac:9c:8e:58:d8:a8:88:b4:d2:fa

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

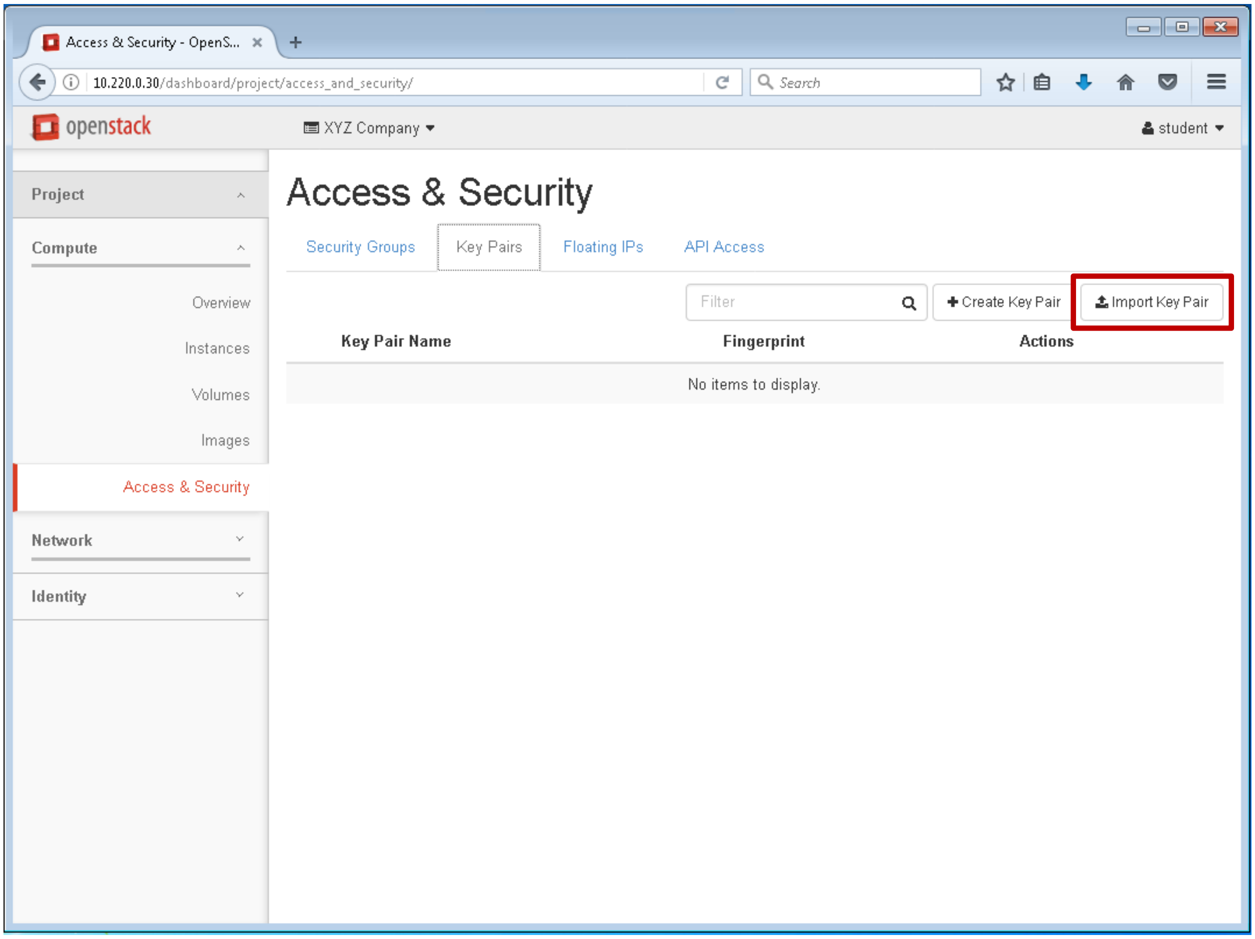
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

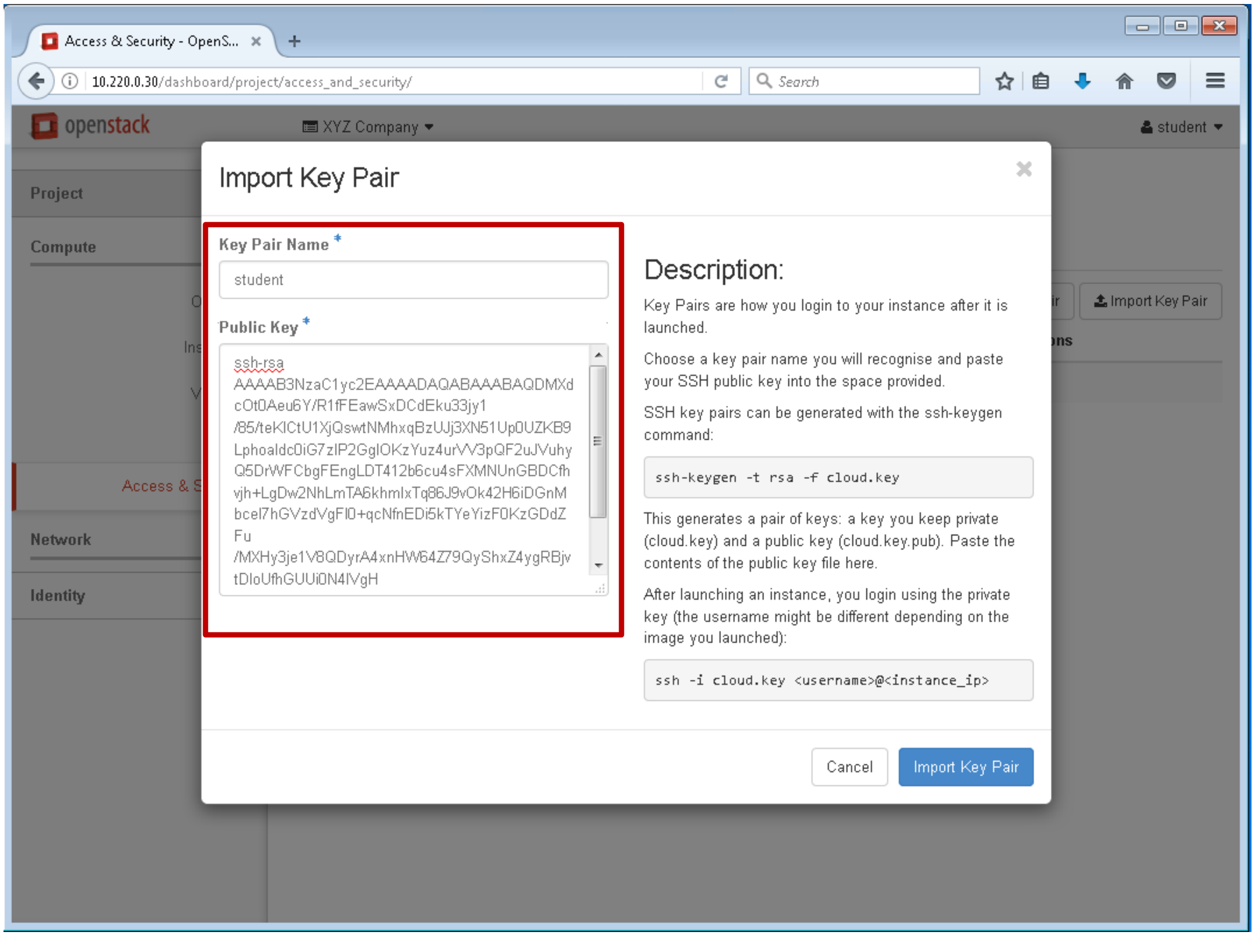
9. **Highlight** and **copy** the **Public key for pasting into OpenSSH authorized_keys file:** as shown in the screen capture.

   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.



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



Import Key Pair

Key Pair Name *

student

Public Key *

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDMXd
cOt0Aeu6Y/R1fFEawSxDCdEku33jy1
/85/teKlCtU1XjQswtNMhxqBzUJj3XN51Up0UZKB9
Lphoaldc0iG7zIP2GglOKzYuz4urVV3pQF2uJVuhy
Q5DrWFCbgFEngLDT412b6cu4sFXMNUnGBDCfh
vjh+LgDw2NhLmTA6khmlxTq86J9vOk42H6iDGnM
bcel7hGVzdVgFl0+qcNfnEDi5kTYeYizF0KzGDdZ
Fu
/MXHy3je1V8QDyrA4xnHW64Z79QyShxZ4ygRBjv
tDloUfhGUUi0N4lVgH
```

Description:

Key Pairs are how you login to your instance after it is launched.

Choose a key pair name you will recognise and paste your SSH public key into the space provided.

SSH key pairs can be generated with the ssh-keygen command:

```
ssh-keygen -t rsa -f cloud.key
```

This generates a pair of keys: a key you keep private (cloud.key) and a public key (cloud.key.pub). Paste the contents of the public key file here.

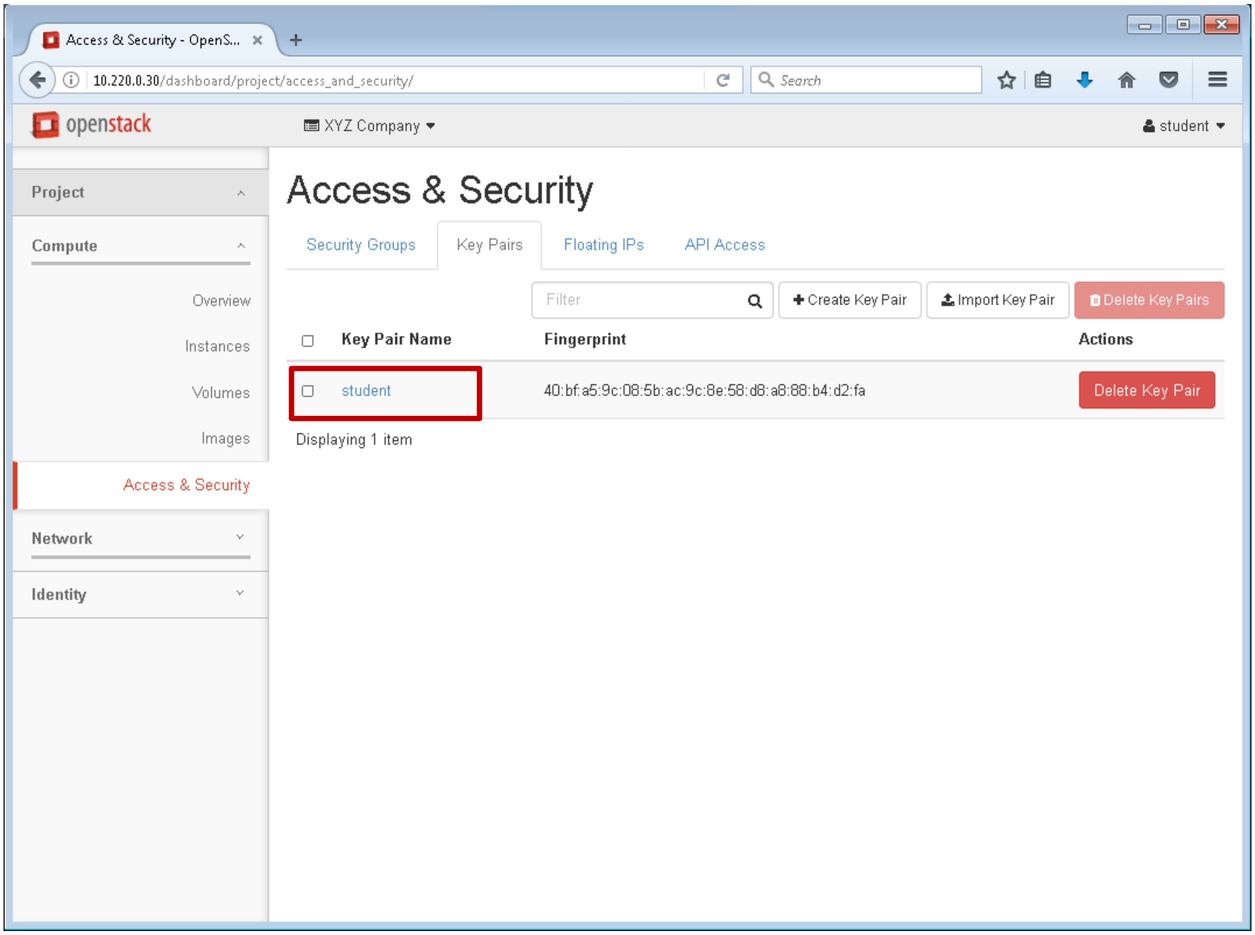
After launching an instance, you login using the private key (the username might be different depending on the image you launched):

```
ssh -i cloud.key <username>@<instance_ip>
```

11. **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**



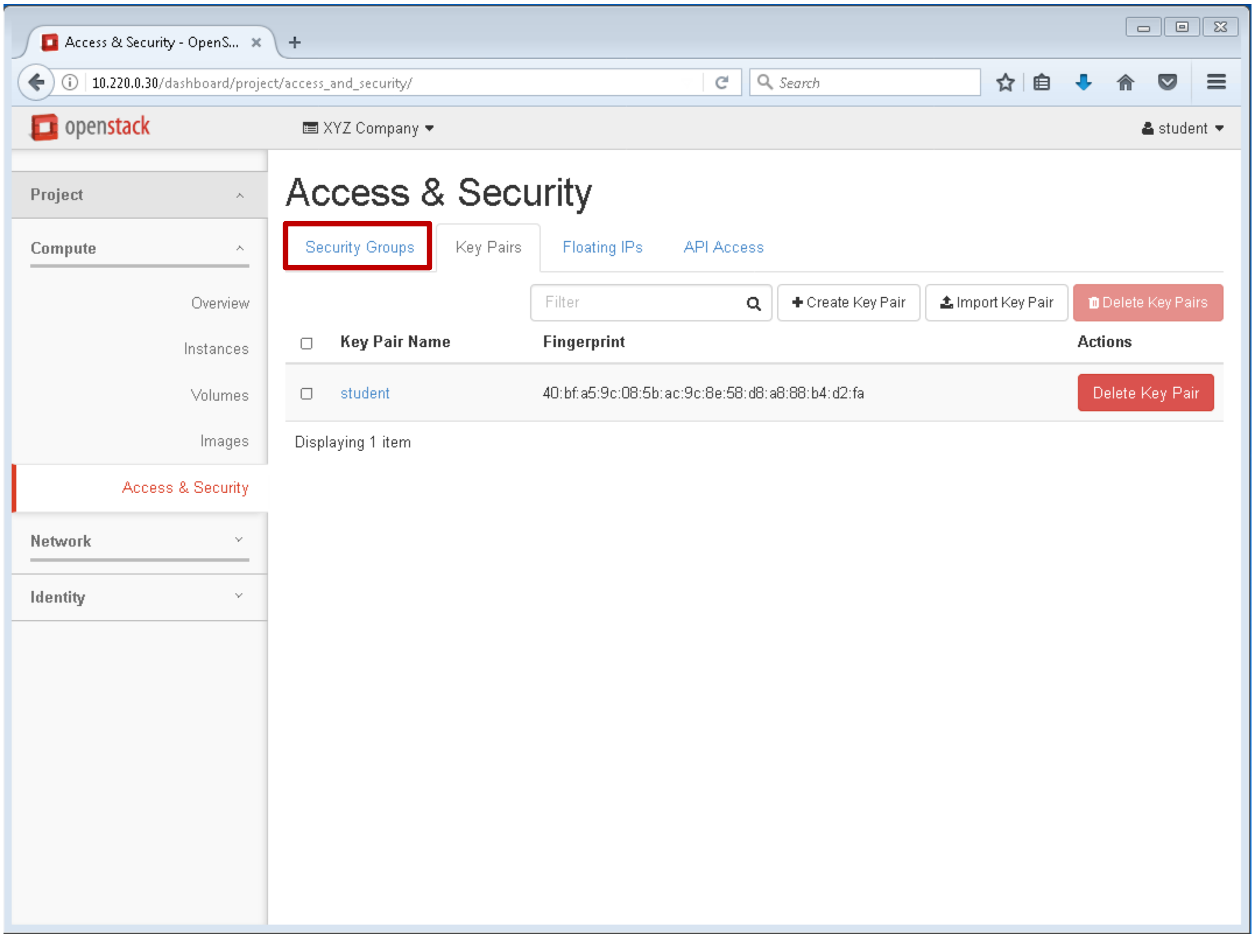
☐	Key Pair Name	Fingerprint	Actions
☐	student	40:bf:a5:9c:08:5b:ac:9c:8e:58:d8:a8:88:b4:d2:fa	Delete Key Pair

Displaying 1 item

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

Continue to Lab 12

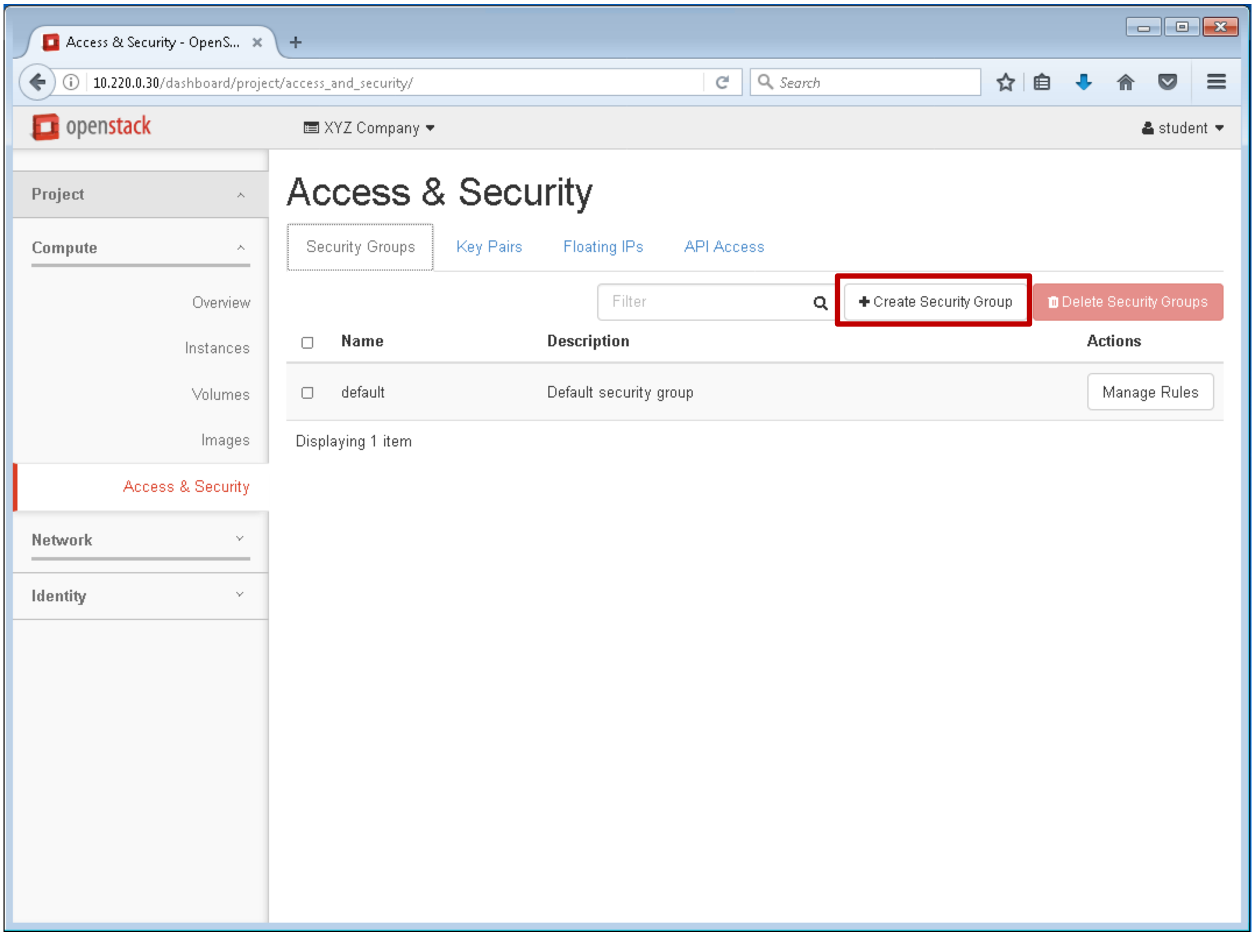
13: Create a Security Group



☐	Key Pair Name	Fingerprint	Actions
☐	student	40:bf:a5:9c:08:5b:ac:9c:8e:58:d8:a8:88:b4:d2:fa	Delete Key Pair

Displaying 1 item

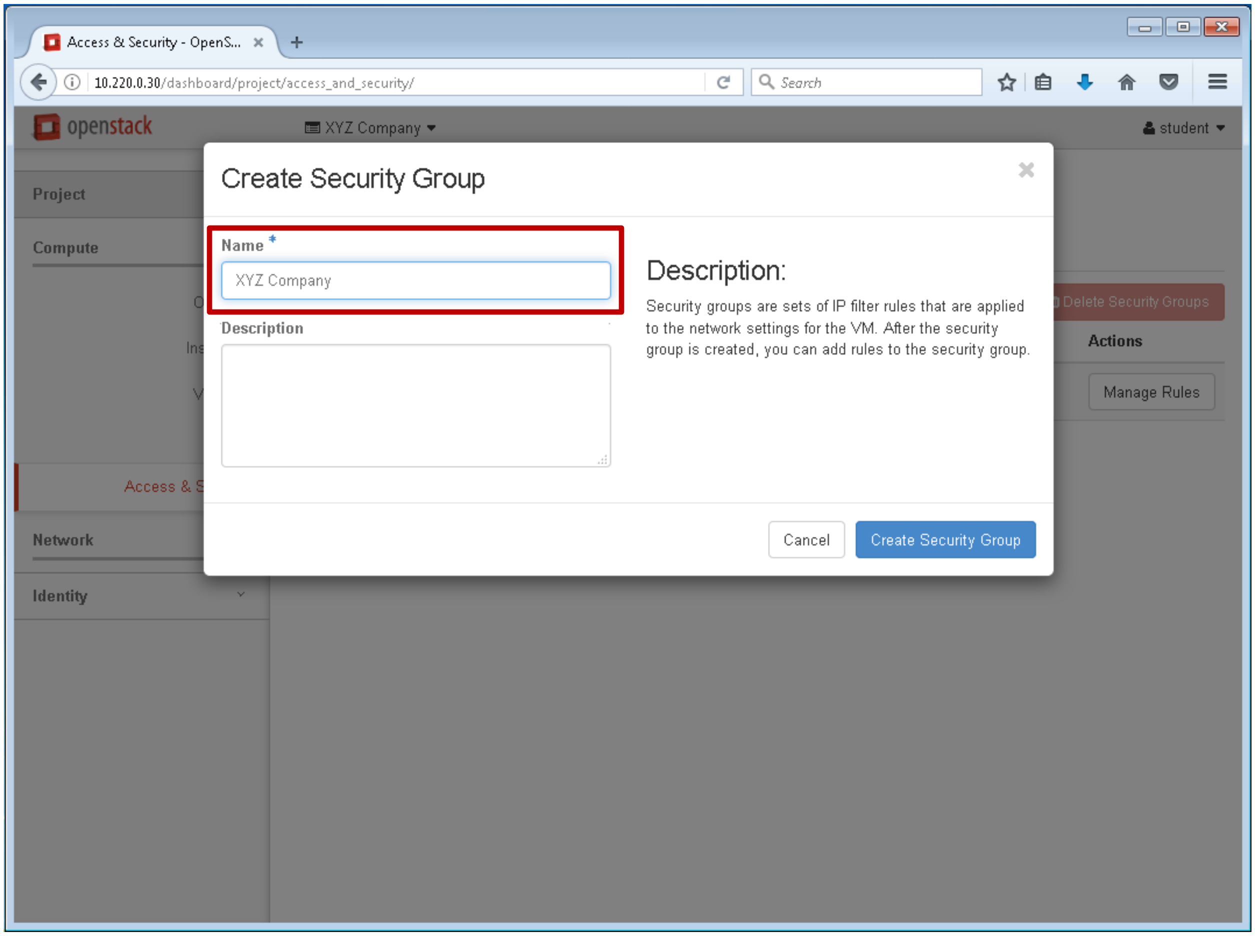
1. **Click** on **Security Groups**



☐	Name	Description	Actions
☐	default	Default security group	Manage Rules

Displaying 1 item

2. **Click** on **Create Security Group**



Name *

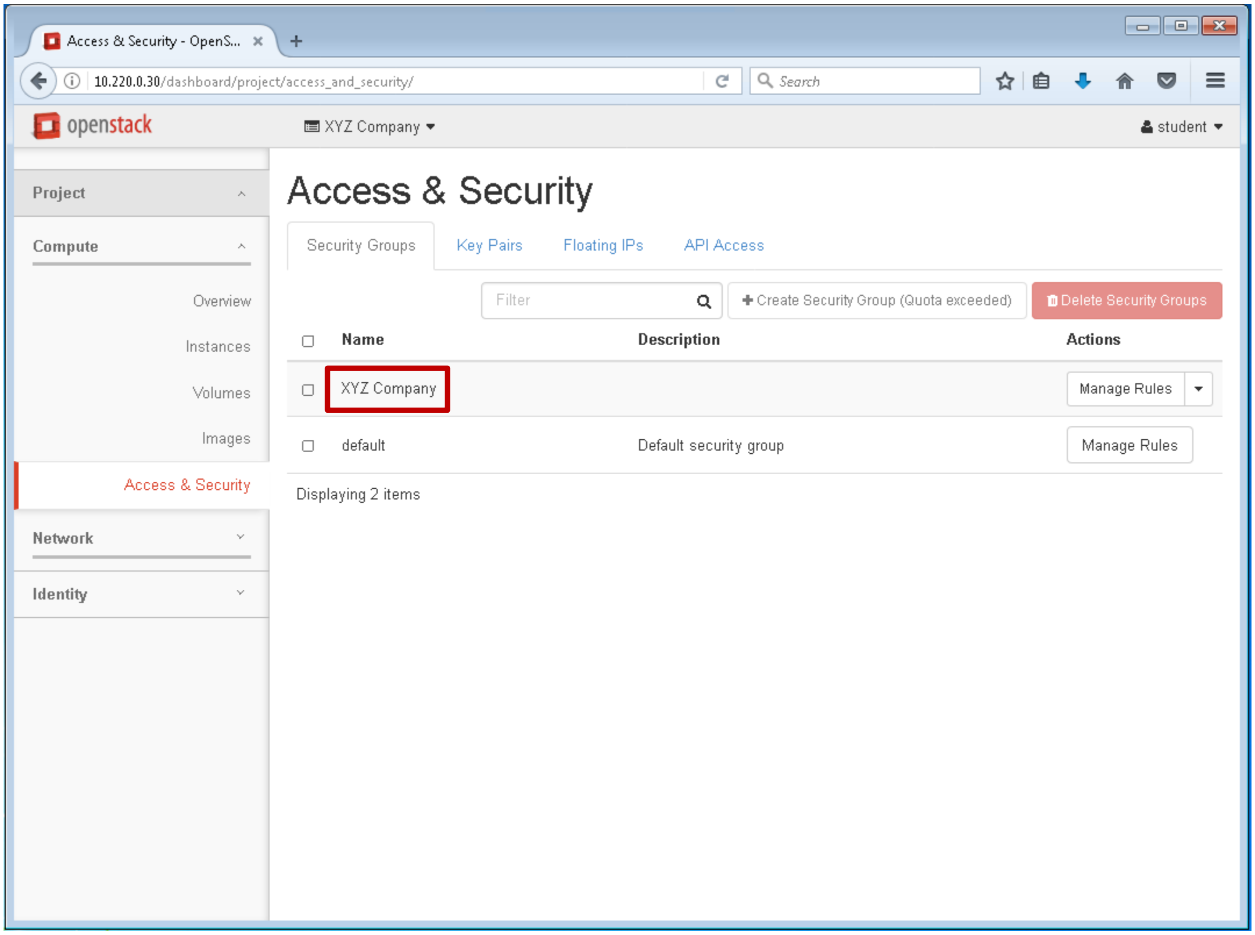
XYZ Company

Description

Description:

Security groups are sets of IP filter rules that are applied to the network settings for the VM. After the security group is created, you can add rules to the security group.

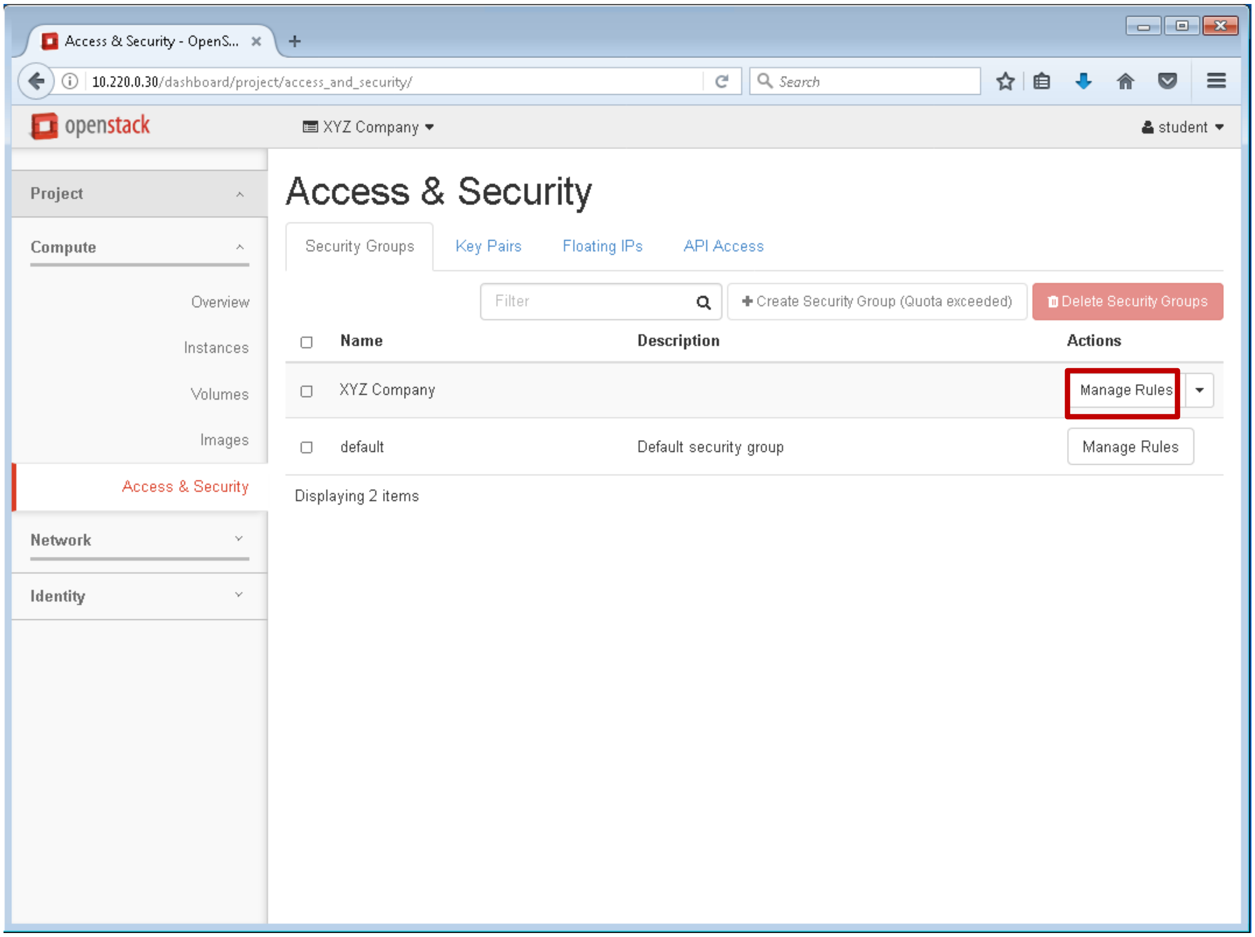
3. **Enter XYZ Company** in the Name block, **Click Create Security Group**



☐	Name	Description	Actions
☐	XYZ Company		Manage Rules
☐	default	Default security group	Manage Rules

Displaying 2 items

4. The XYZ Company should be added as shown



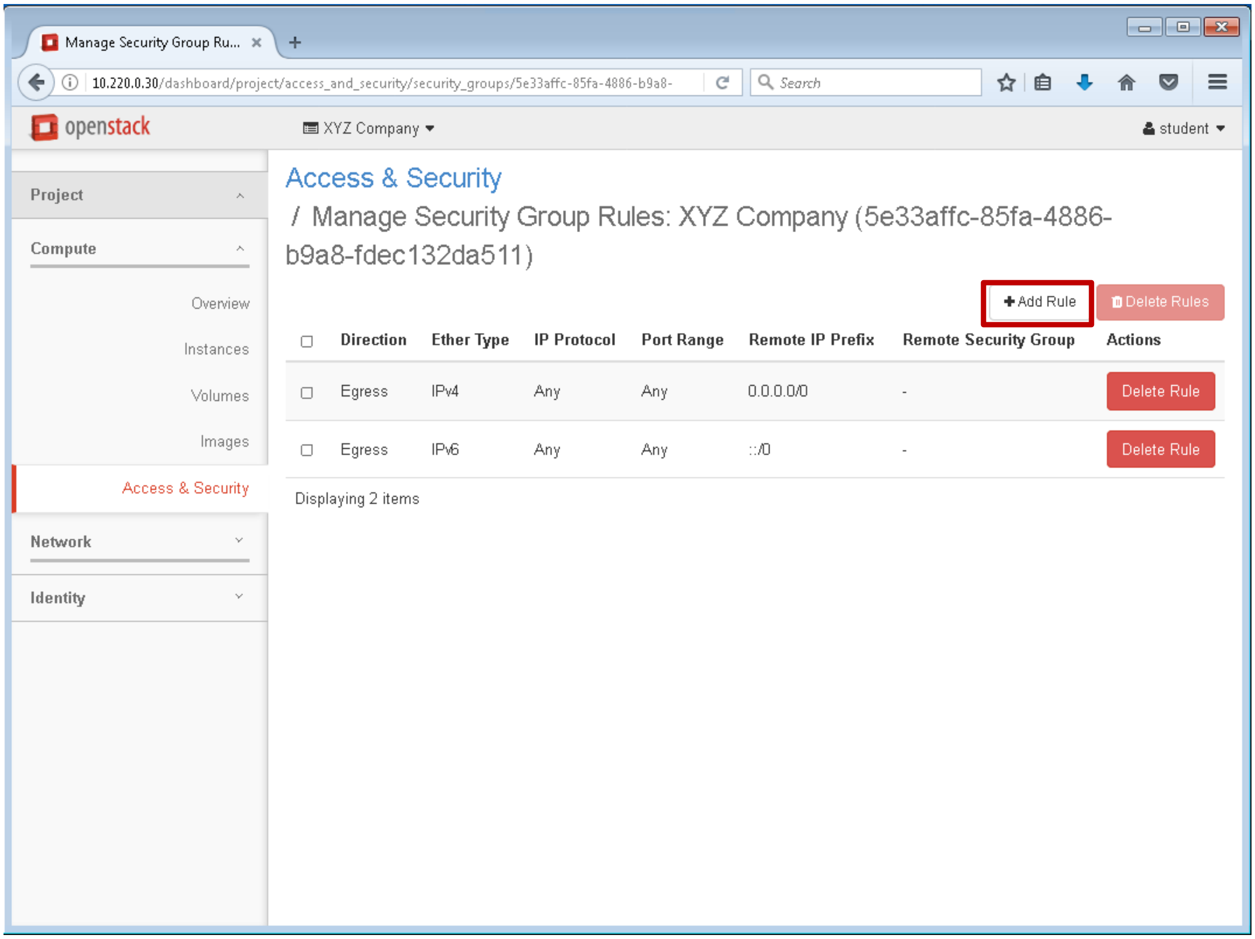
☐	Name	Description	Actions
☐	XYZ Company		Manage Rules
☐	default	Default security group	Manage Rules

Displaying 2 items

5. **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.



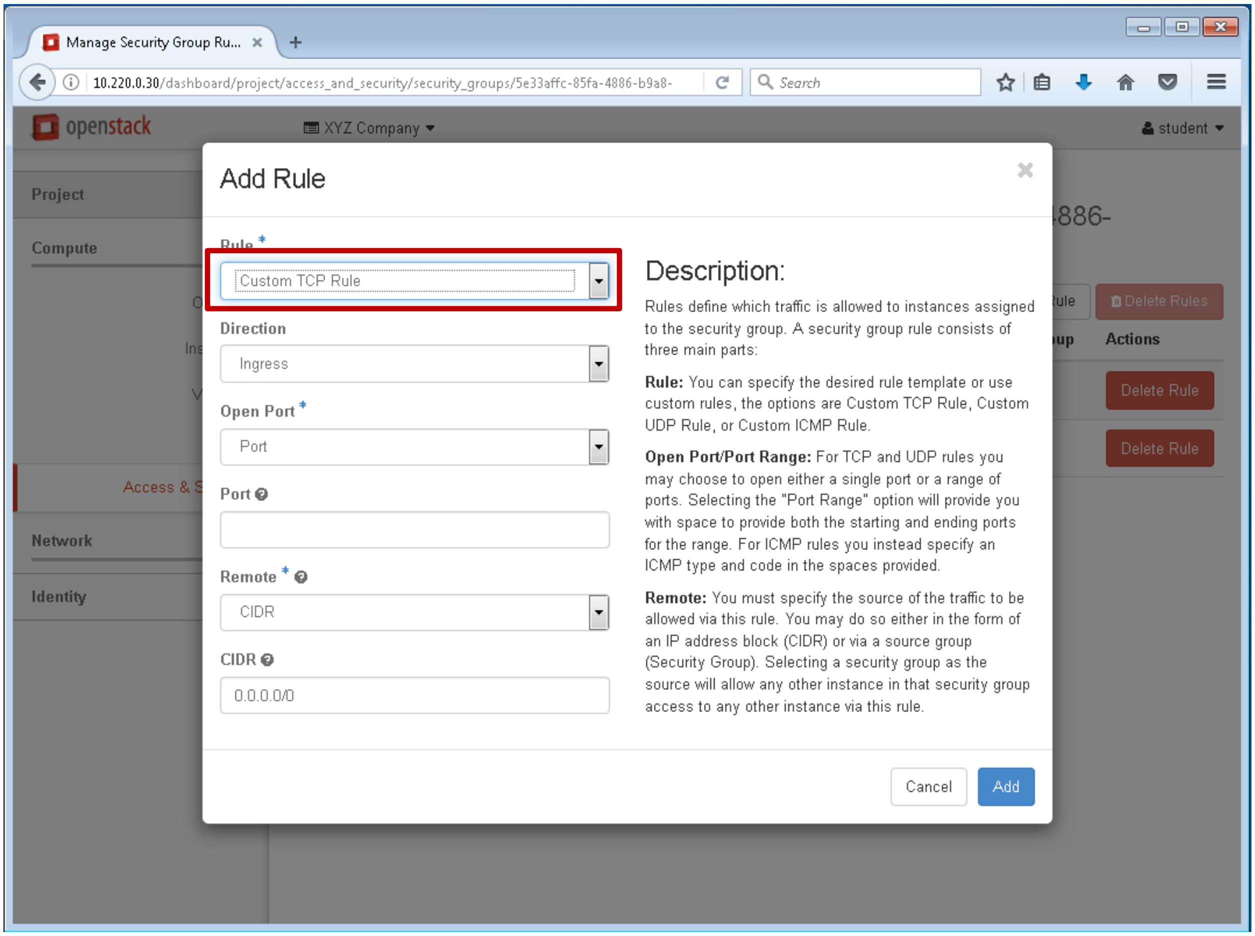
Access & Security

/ Manage Security Group Rules: XYZ Company (5e33affc-85fa-4886-b9a8-fdec132da511)

☐	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
☐	Egress	IPv6	Any	Any	::/0	-	Delete Rule

Displaying 2 items

6. **Click** on **Add Rule**



Add Rule

Rule *: Custom TCP Rule

Direction: Ingress

Open Port *: Port

Port:

Remote *: CIDR

CIDR: 0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

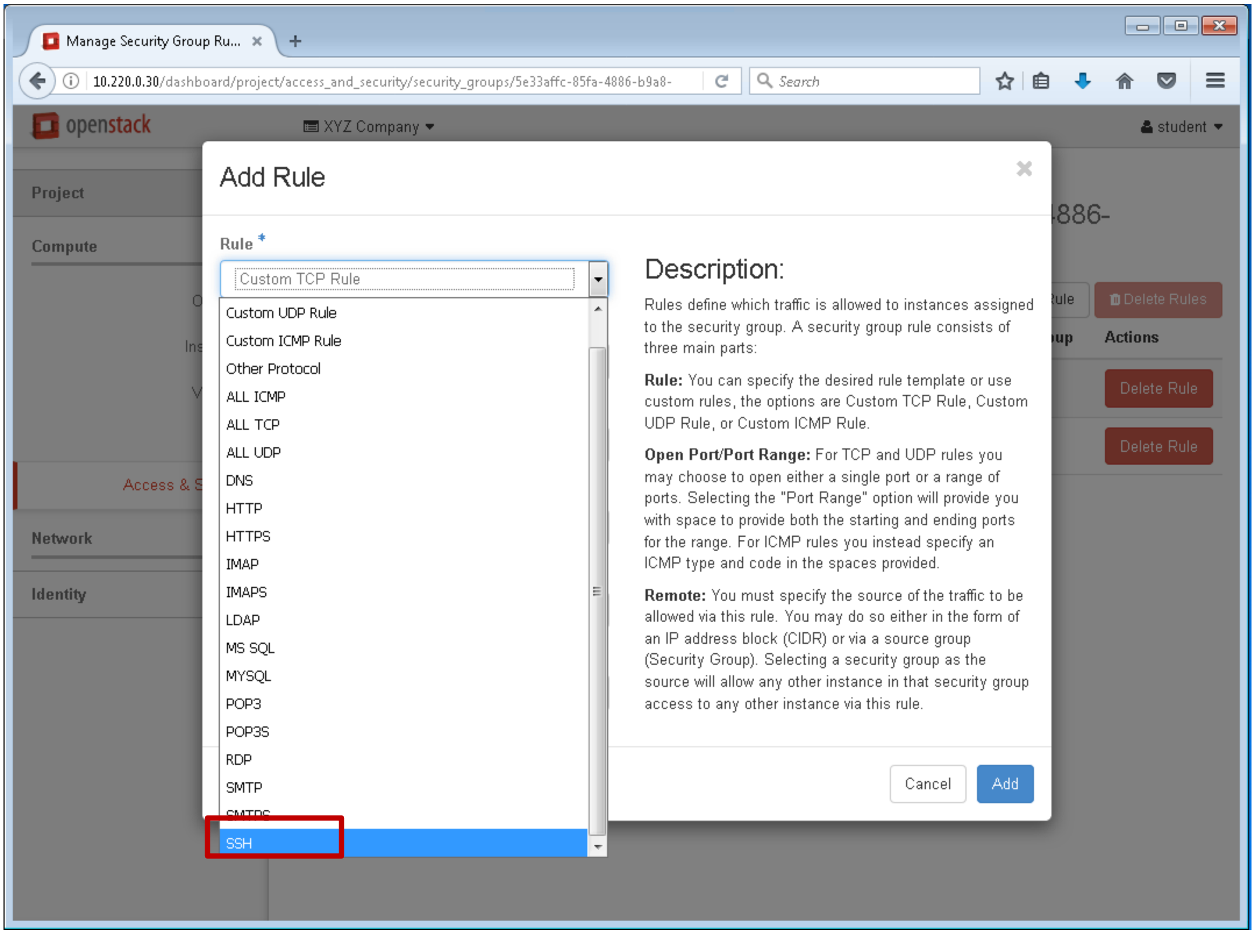
Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

7. **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.



Description:

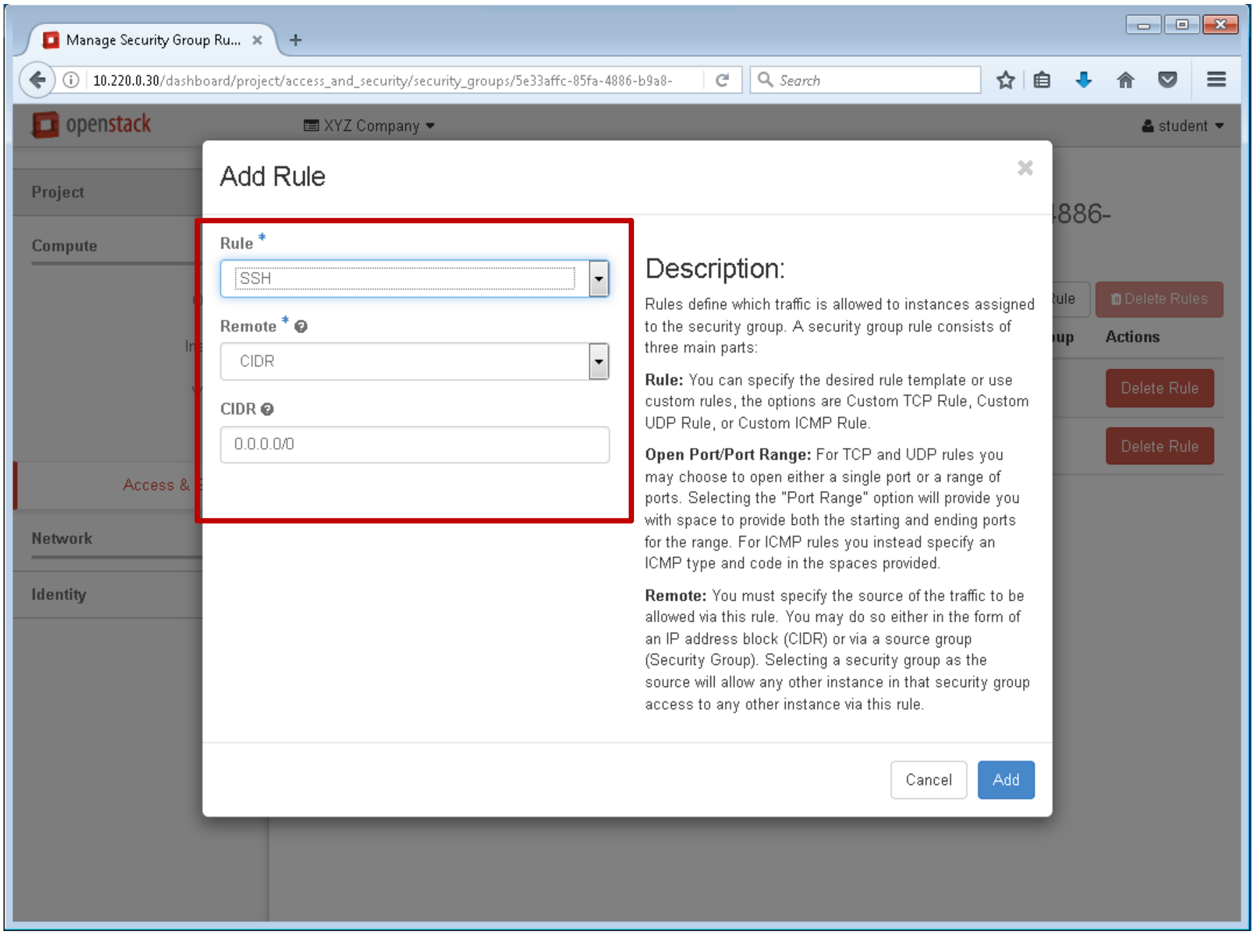
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

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



Add Rule

Rule *: SSH

Remote *: CIDR

CIDR: 0.0.0.0/0

Description:

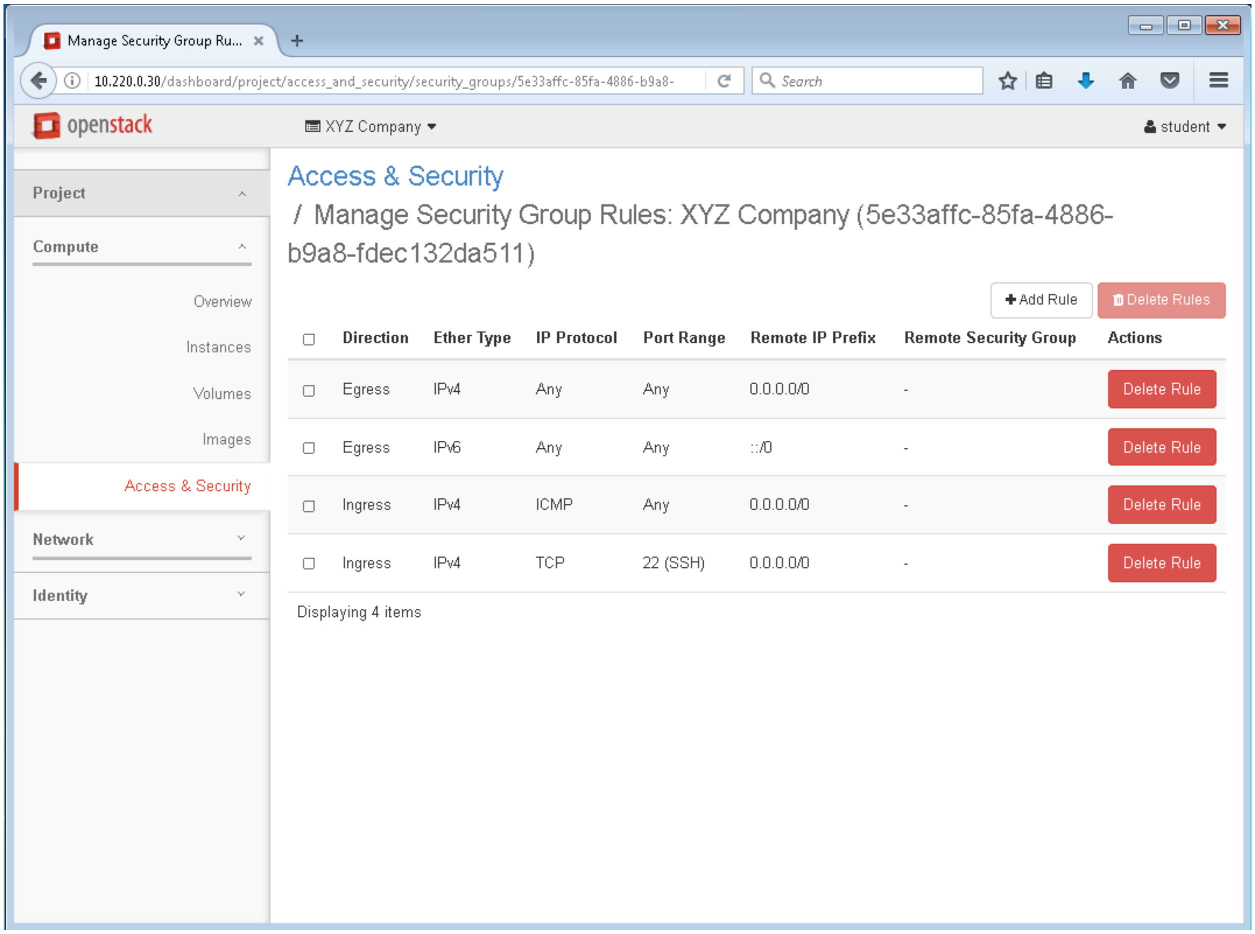
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

9. 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

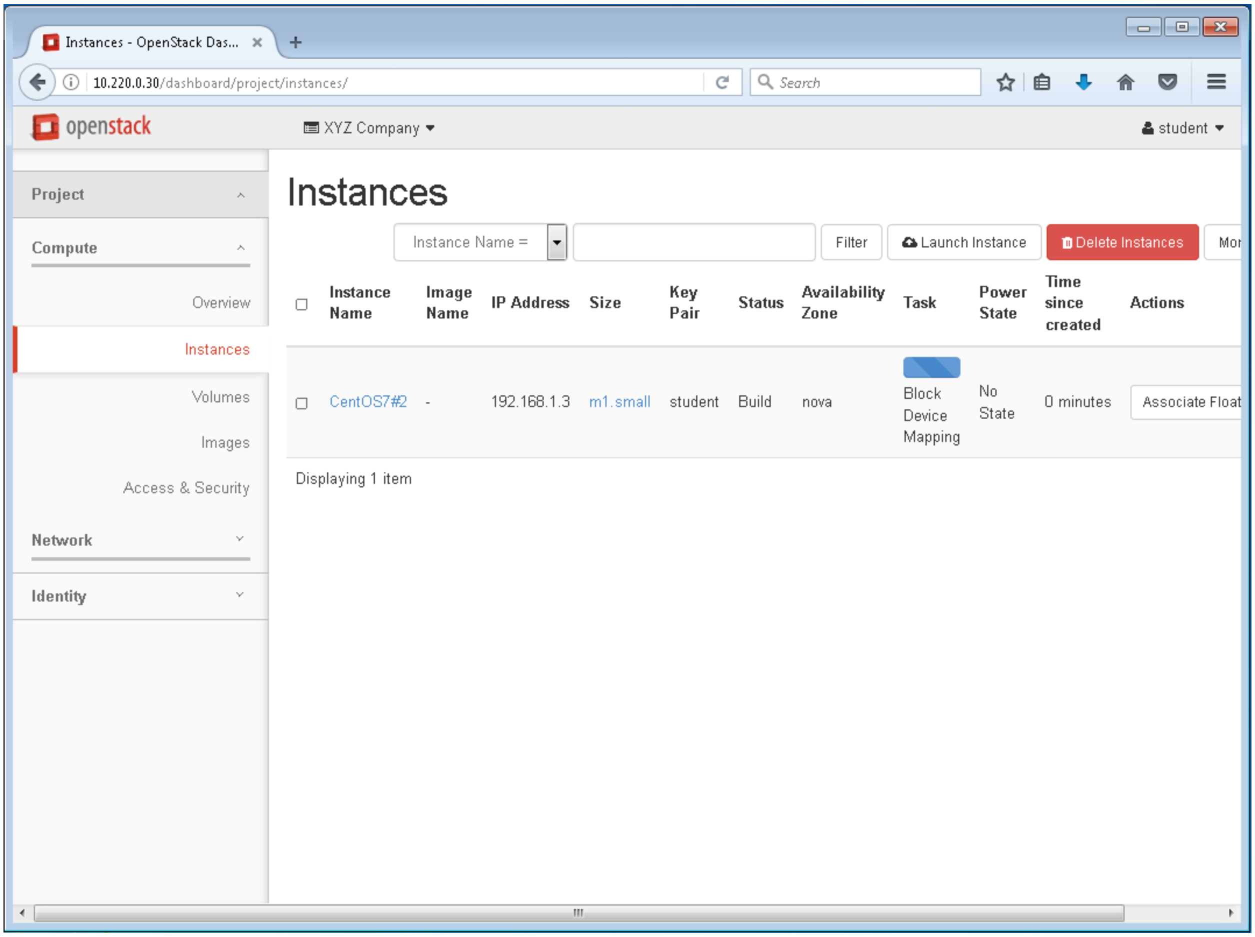


Access & Security / Manage Security Group Rules: XYZ Company (5e33affc-85fa-4886-b9a8-fdec132da511)

☐	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
☐	Egress	IPv6	Any	Any	::/0	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	Delete Rule
☐	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	Delete Rule

Displaying 4 items

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

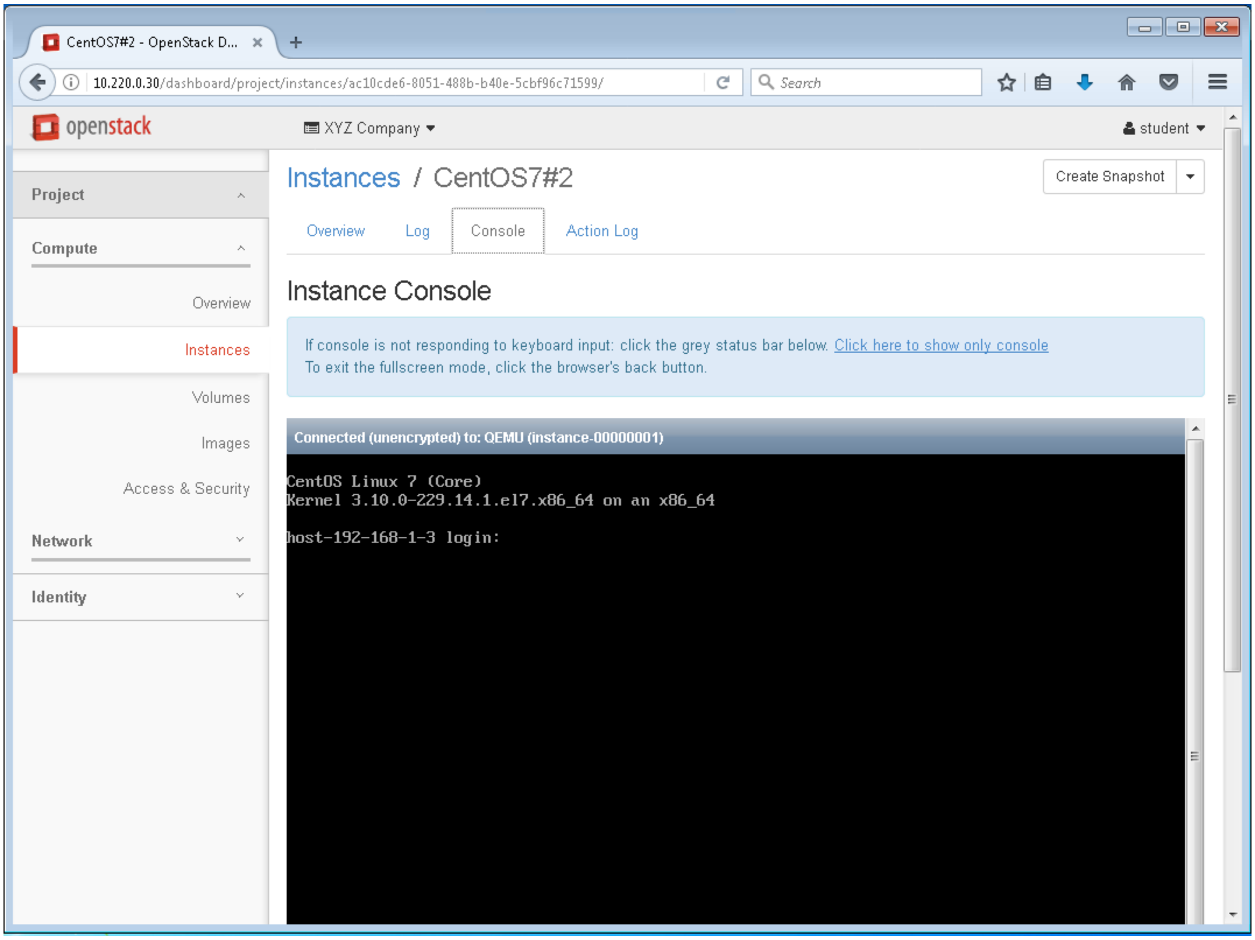


☐	Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
☐	CentOS7#2	-	192.168.1.3	m1.small	student	Build	nova	Block Device Mapping	No State	0 minutes	Associate Float

Displaying 1 item

11. 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



Instances / CentOS7#2

Instance Console

If console is not responding to keyboard input: click the grey status bar below. Click here to show only console
To exit the fullscreen mode, click the browser's back button.

Connected (unencrypted) to: QEMU (instance-00000001)

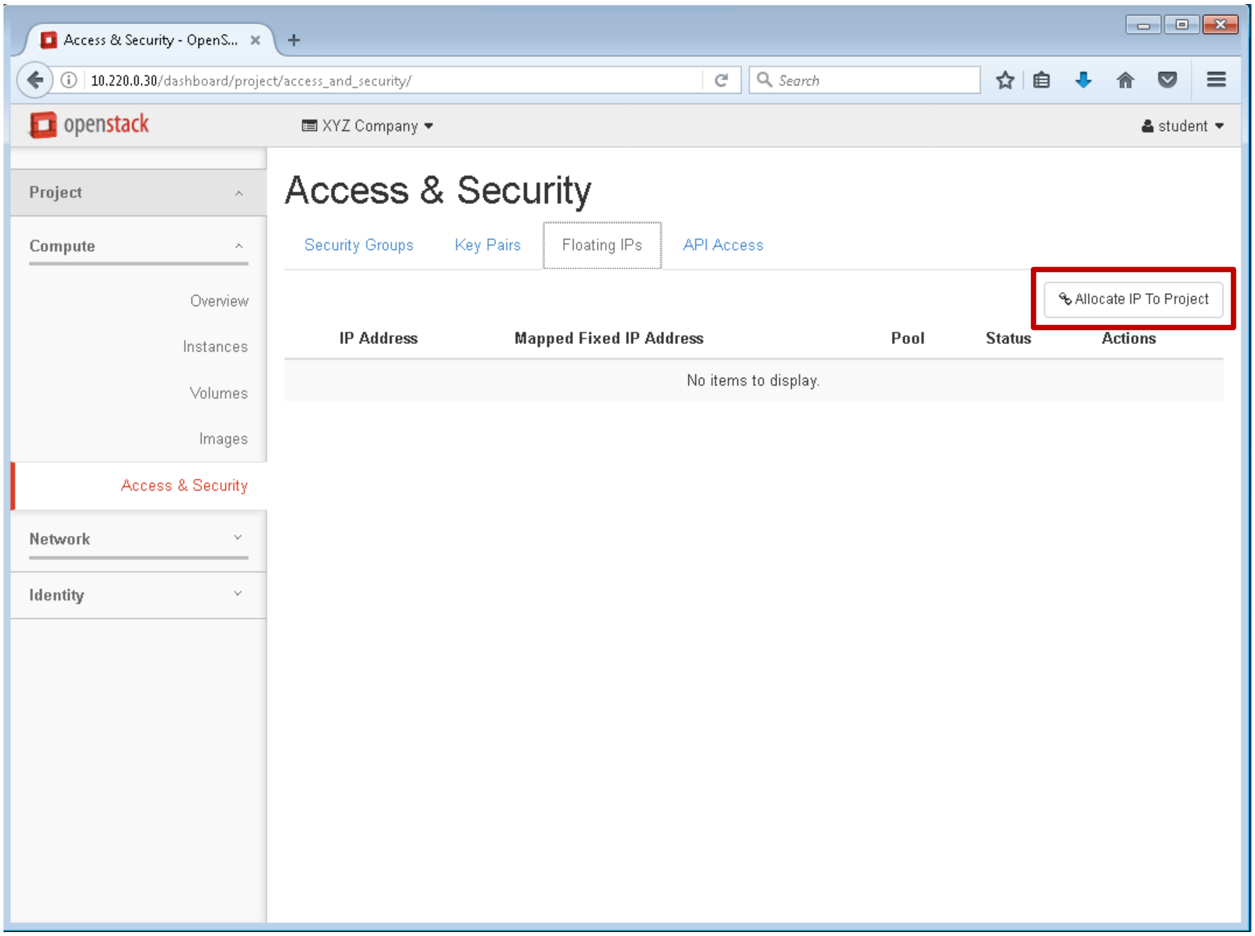
```
CentOS Linux 7 (Core)
Kernel 3.10.0-229.14.1.el7.x86_64 on an x86_64

host-192-168-1-3 login:
```

12. 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

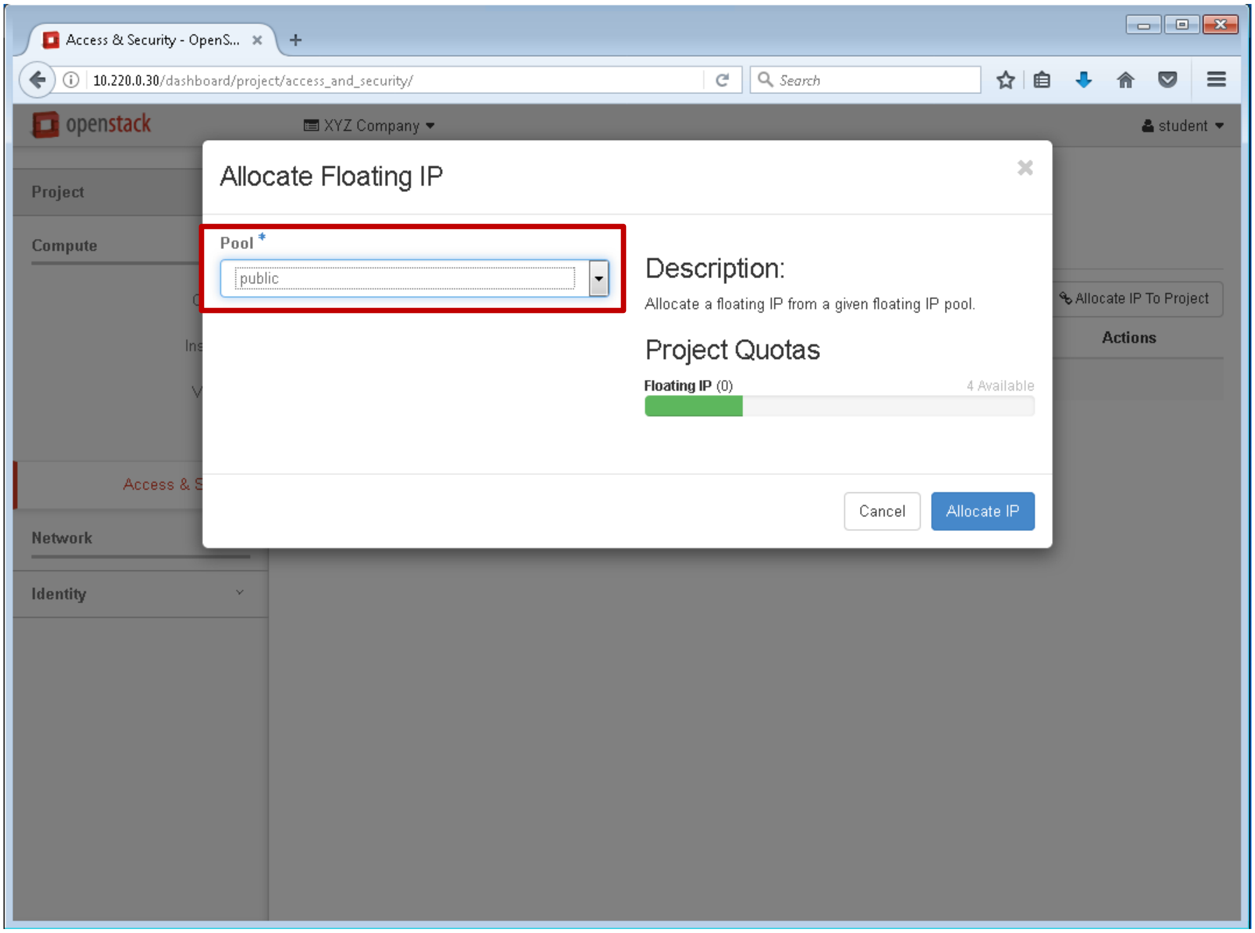
Lab 13: Allocate and Associate a Floating IP Address to an OpenStack CentOS 7 Instance.



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.



Allocate Floating IP

Pool * public

Description:

Allocate a floating IP from a given floating IP pool.

Project Quotas

Floating IP (0) 4 Available

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

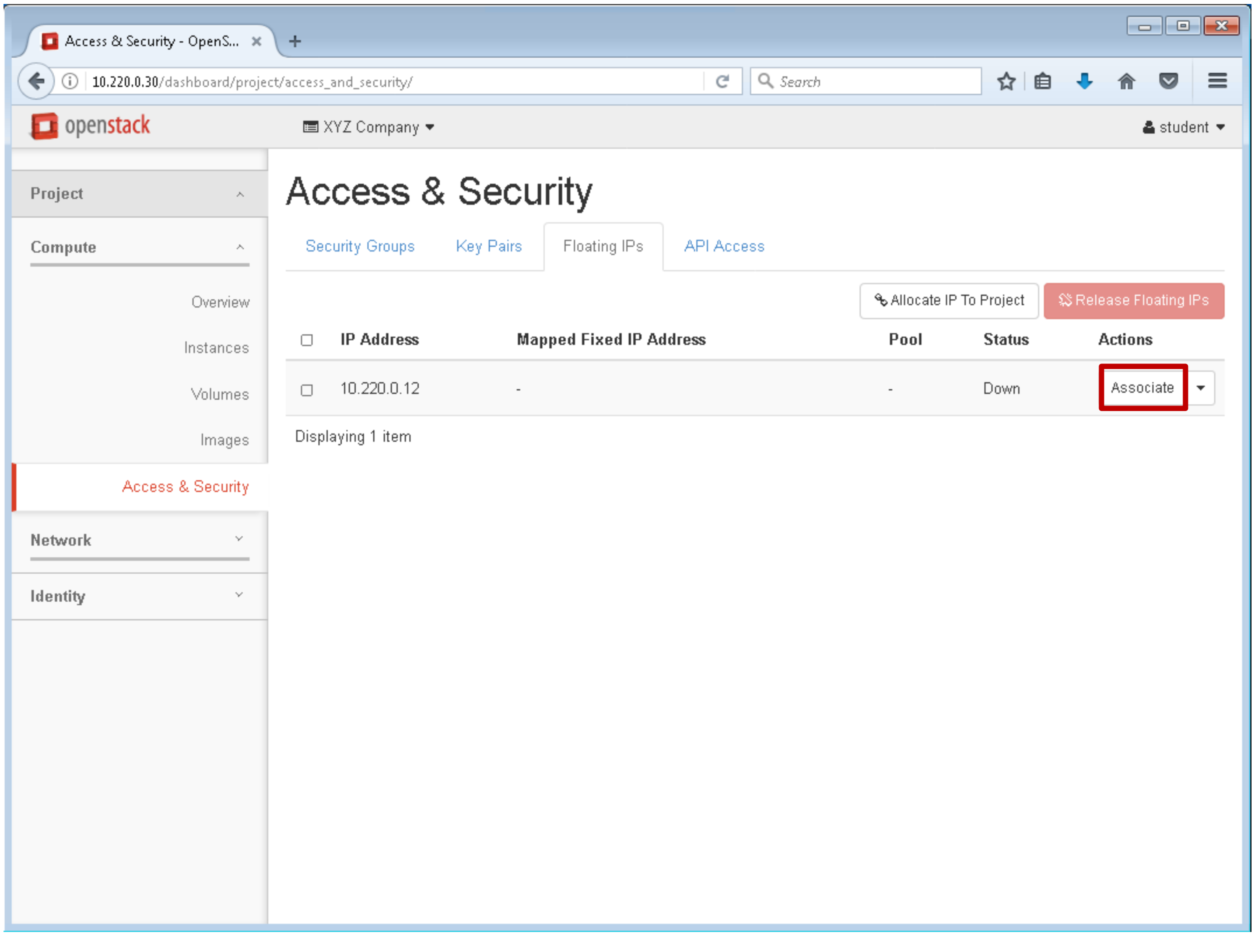
Routable IP Addresses

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



Access & Security

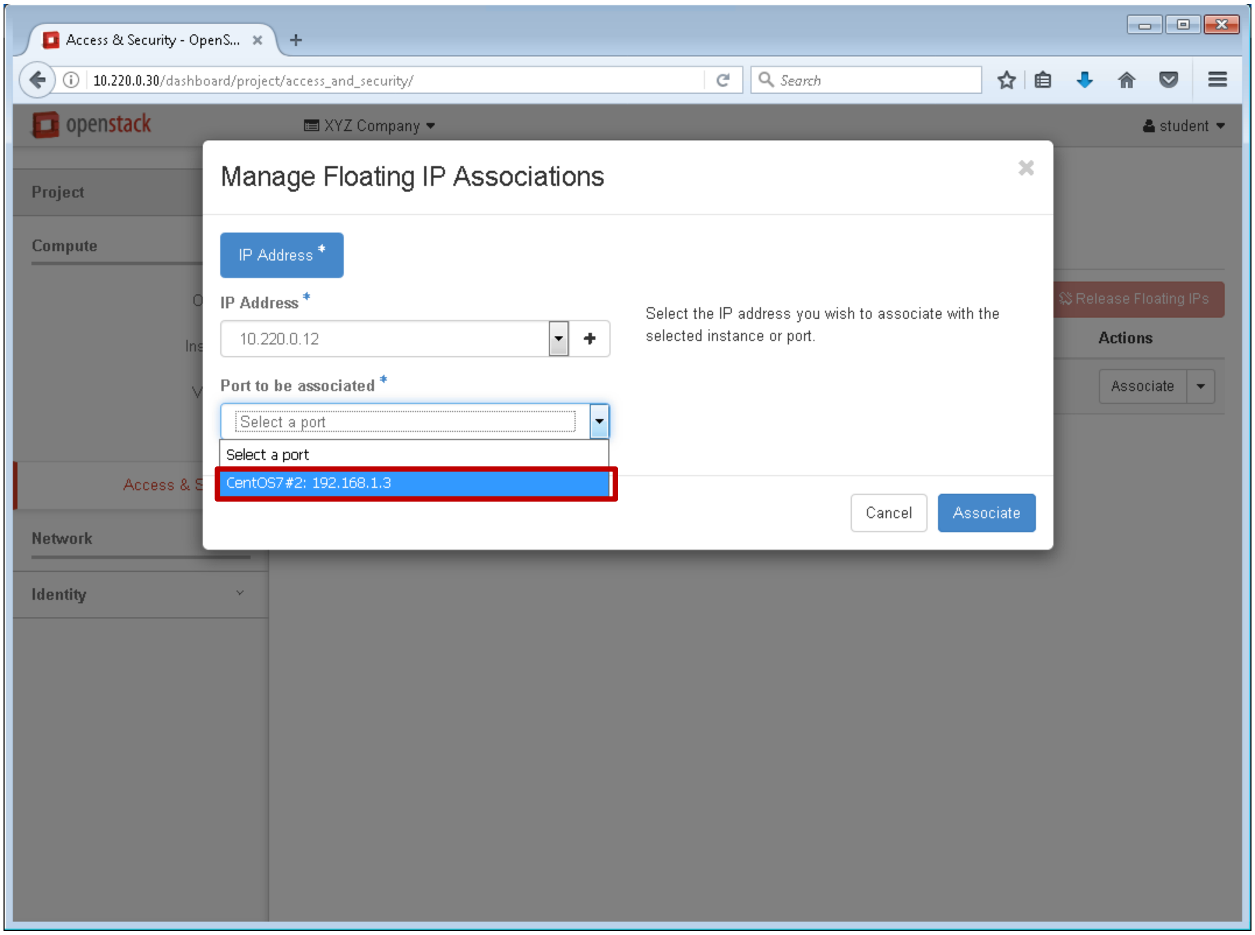
☐	IP Address	Mapped Fixed IP Address	Pool	Status	Actions
☐	10.220.0.12	-	-	Down	Associate

Displaying 1 item

3. 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.



IP Address *: 10.220.0.12

Port to be associated *: Select a port

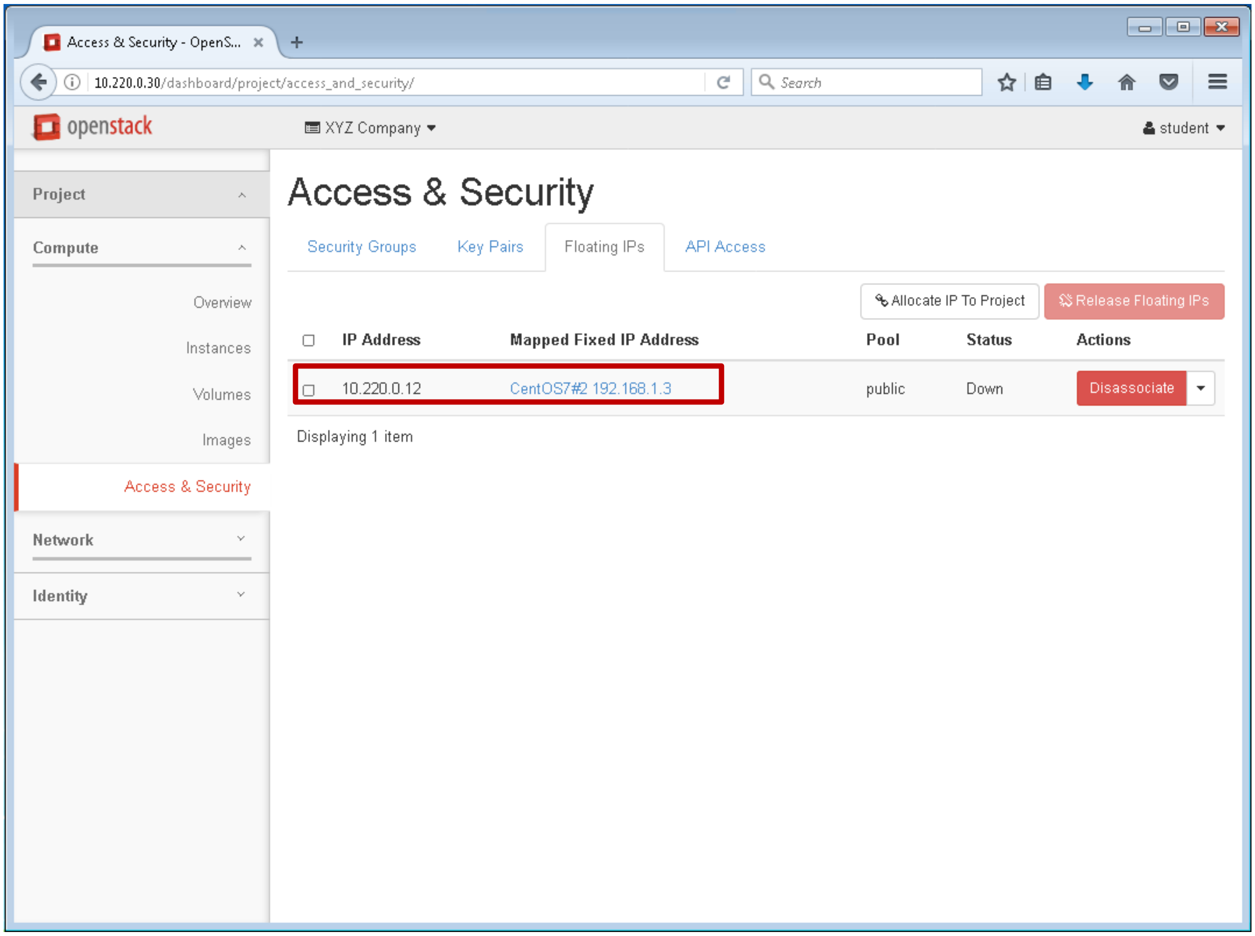
Select a port
CentOS7#2: 192.168.1.3

Select the IP address you wish to associate with the selected instance or port.

4. 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.



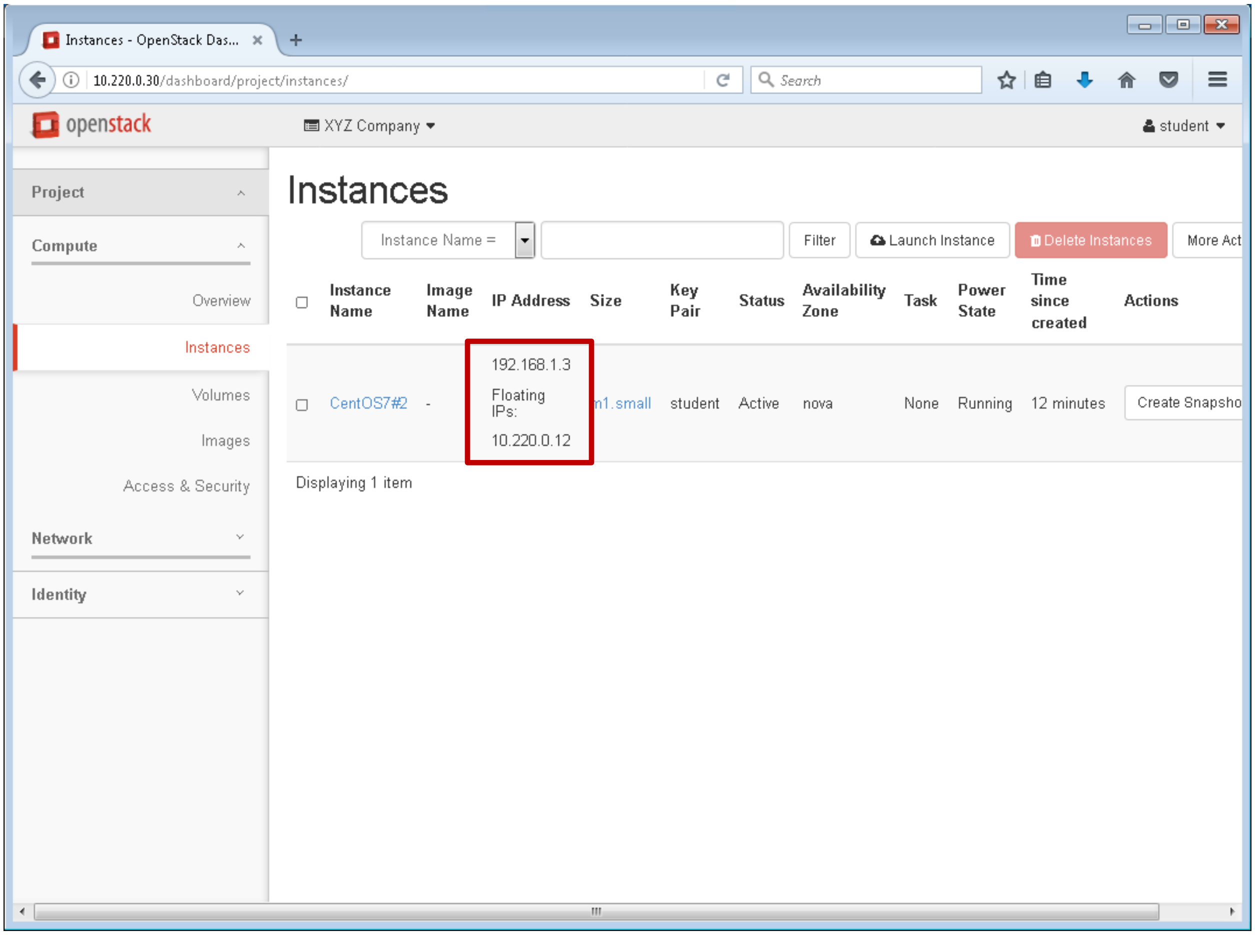
☐	IP Address	Mapped Fixed IP Address	Pool	Status	Actions
☐	10.220.0.12	CentOS7#2 192.168.1.3	public	Down	Disassociate

Displaying 1 item

5. **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.



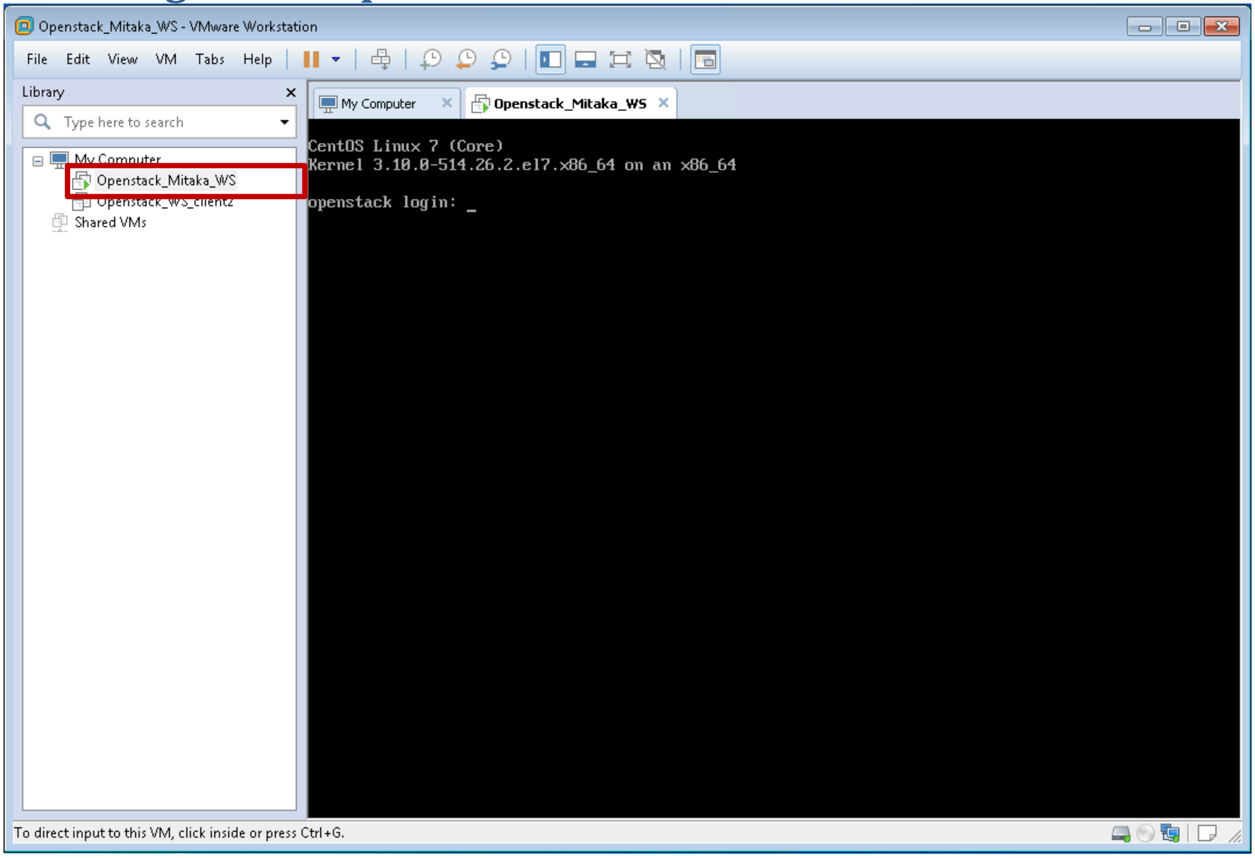
☐	Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
☐	CentOS7#2	-	192.168.1.3 Floating IPs: 10.220.0.12	m1.small	student	Active	nova	None	Running	12 minutes	Create Snapsho

Displaying 1 item

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

Continue to Grade Script

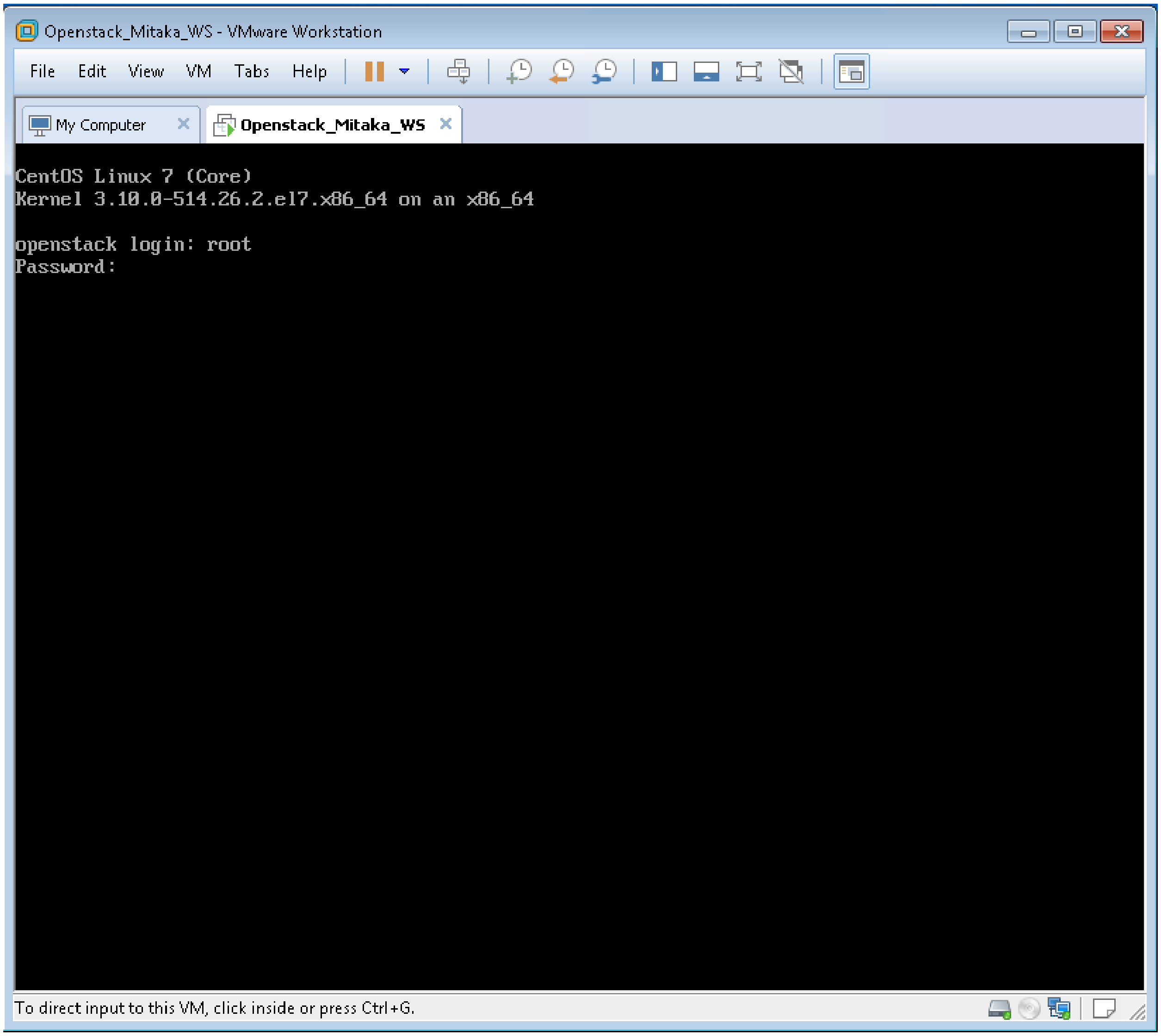
Run the grade script


Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Openstack_Mitaka_WS
Openstack_WS_client2
Shared VMs
My Computer
Openstack_Mitaka_WS
To direct input to this VM, click inside or press Ctrl+G.

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

openstack login: _
```

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

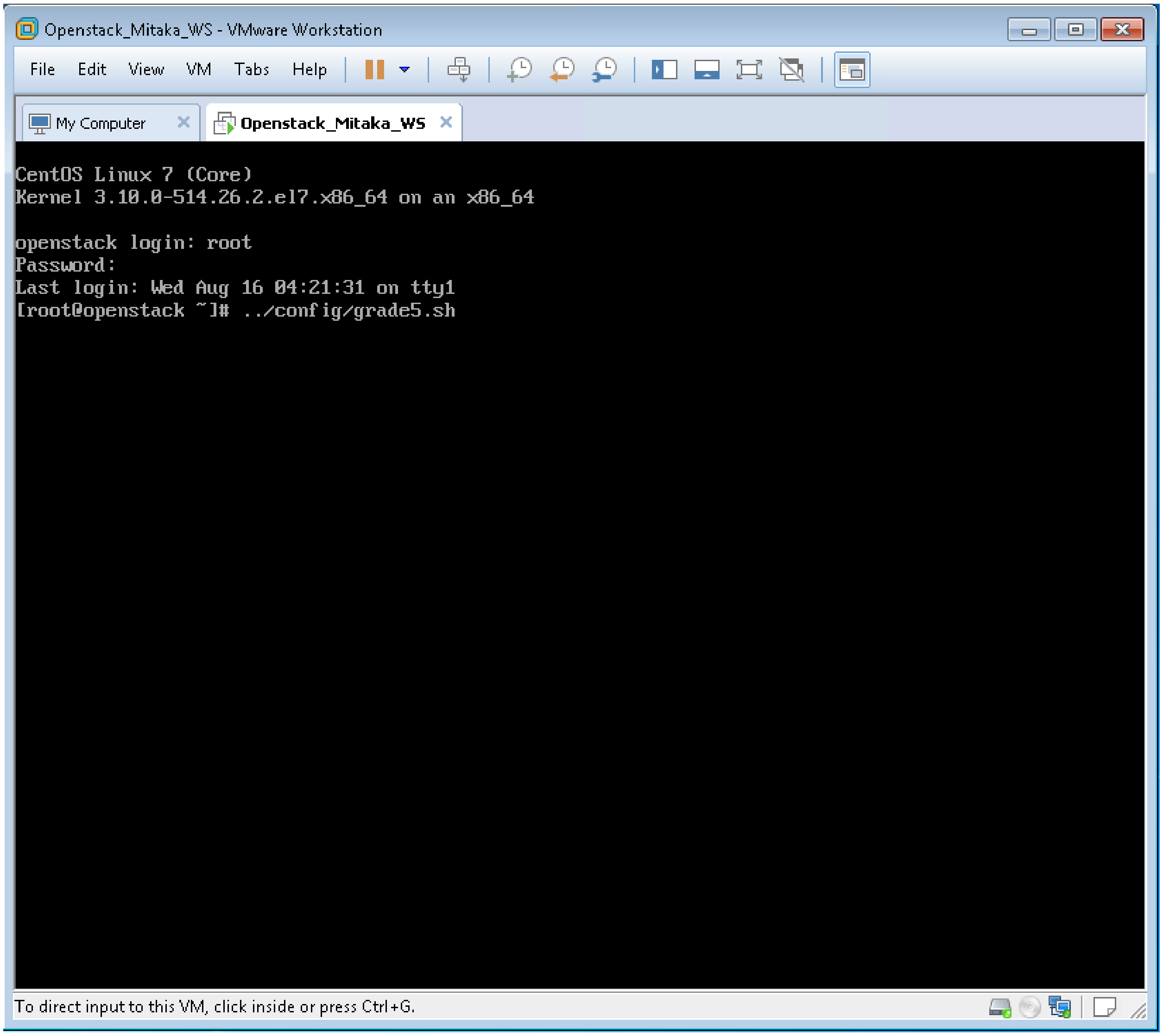
   Note: The OpenStack_Mitaka_WS console may still be open on your desktop from when you ran the setup script


Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
My Computer
Openstack_Mitaka_WS
To direct input to this VM, click inside or press Ctrl+G.

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

openstack login: root
Password:
```

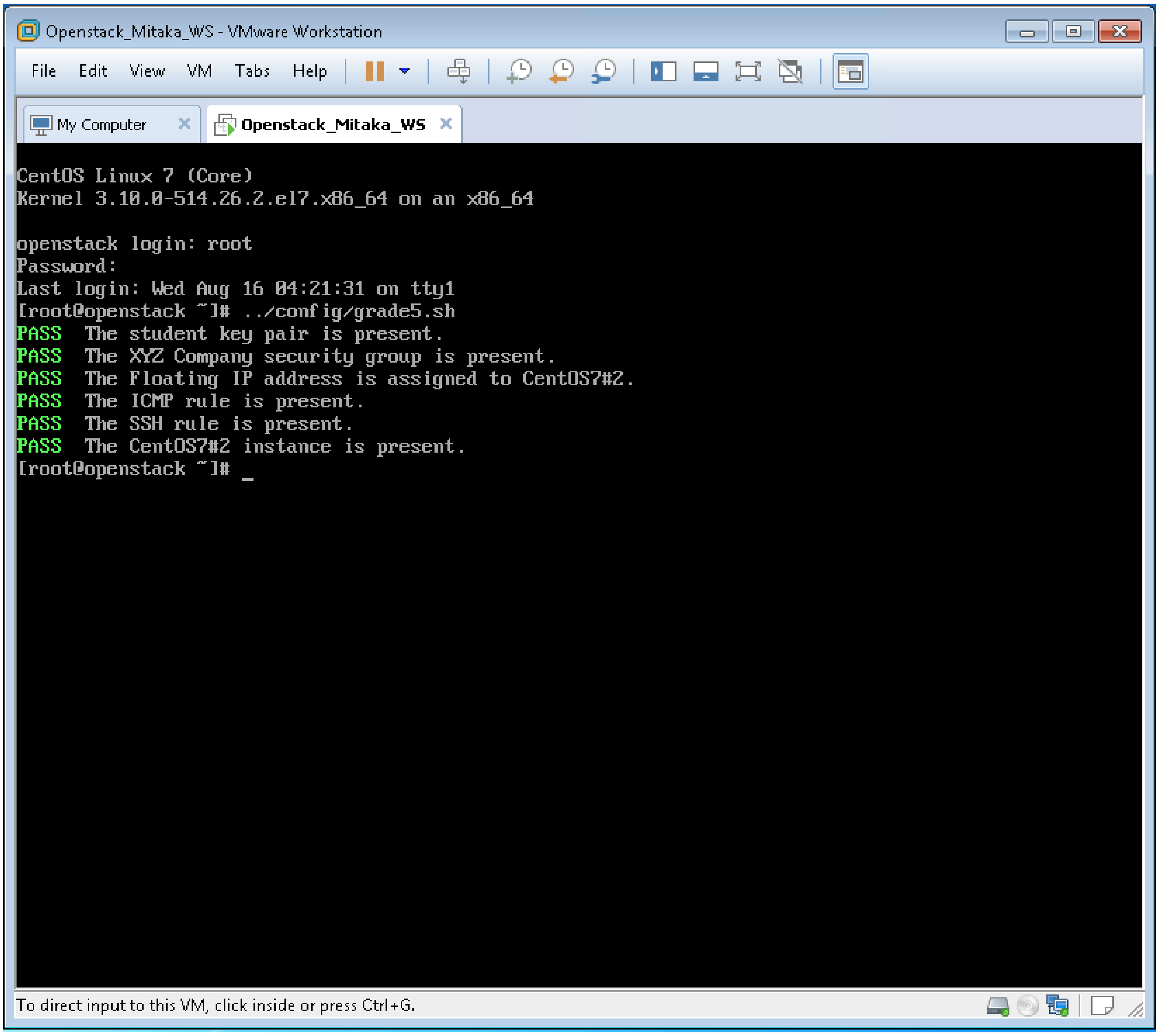
2. Log in as root with the Password: P@ssword

   Note: The password is NOT visible as you type it


Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
My Computer
Openstack_Mitaka_WS
To direct input to this VM, click inside or press Ctrl+G.

```
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 04:21:31 on tty1
[root@openstack ~]# ../config/grade5.sh
```

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


Openstack_Mitaka_WS - VMware Workstation
File Edit View VM Tabs Help
My Computer
Openstack_Mitaka_WS
To direct input to this VM, click inside or press Ctrl+G.

```
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 04:21:31 on tty1
[root@openstack ~]# ../config/grade5.sh
PASS  The student key pair is present.
PASS  The XYZ Company security group is present.
PASS  The Floating IP address is assigned to CentOS7#2.
PASS  The ICMP rule is present.
PASS  The SSH rule is present.
PASS  The CentOS7#2 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_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.