**Lab 3: Advanced OpenStack Operations**



# Objectives:

In this lab, we will investigate some frequently-used OpenStack operations. Besides the simple and straightforward VM launch with a testing system Cirros, you can customize more settings to build a ready-to-use production VM in order to deploy your applications.

You will learn the following skills: (1) upload new images to the OpenStack server; (2) define and modify your customized security group; (3) create key pairs for VMs; (4) Launch and SSH to your VMs.

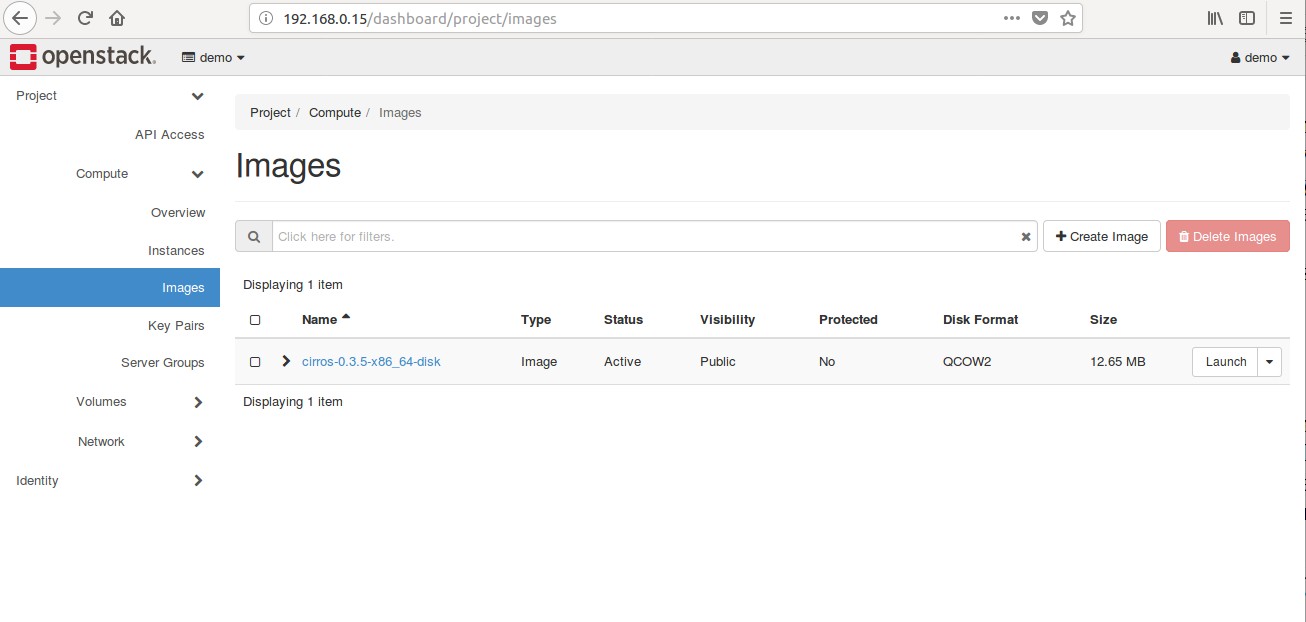
# Upload new images to OpenStack

You have already found that there is only one small “cirros” image offered by DevStack, which is for testing purpose without much production ability. How to add new images to your OpenStack such as Ubuntu, CentOS and even Windows? You may need these operating systems to make software development, deploy applications or do programming test for your homeworks. : )

Fortunately, OpenStack does prepare such function for us.

## Let’s check the image list

Please log in your OpenStack using “demo” username. Then click “Compute” and choose “Images” tag, the available images are listed on screen.

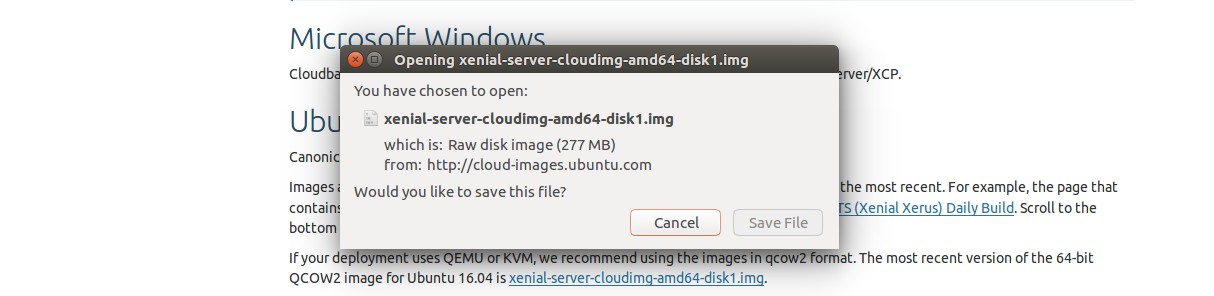


## Download a new image.

Check the website: <https://docs.openstack.org/image-guide/obtain-images.html> The OpenStack official website offers us many options:

* + CentOS
  + Cirros
  + Debian
  + Fedora
  + Microsoft Windows
  + Ubuntu
  + openSUSE and SUSE Linux
  + Enterprise Server
  + Red Had Enterprise Linux

Here we download an Ubuntu-based image named “xenial-server-cloudimg-amd64-disk1.img” for our lab. Click the link and a download window will pop up. You can save the file anywhere you remember.



## Create a new image.

Go back to the image page in step 1. Click “+ Create Image”. You will see the following:

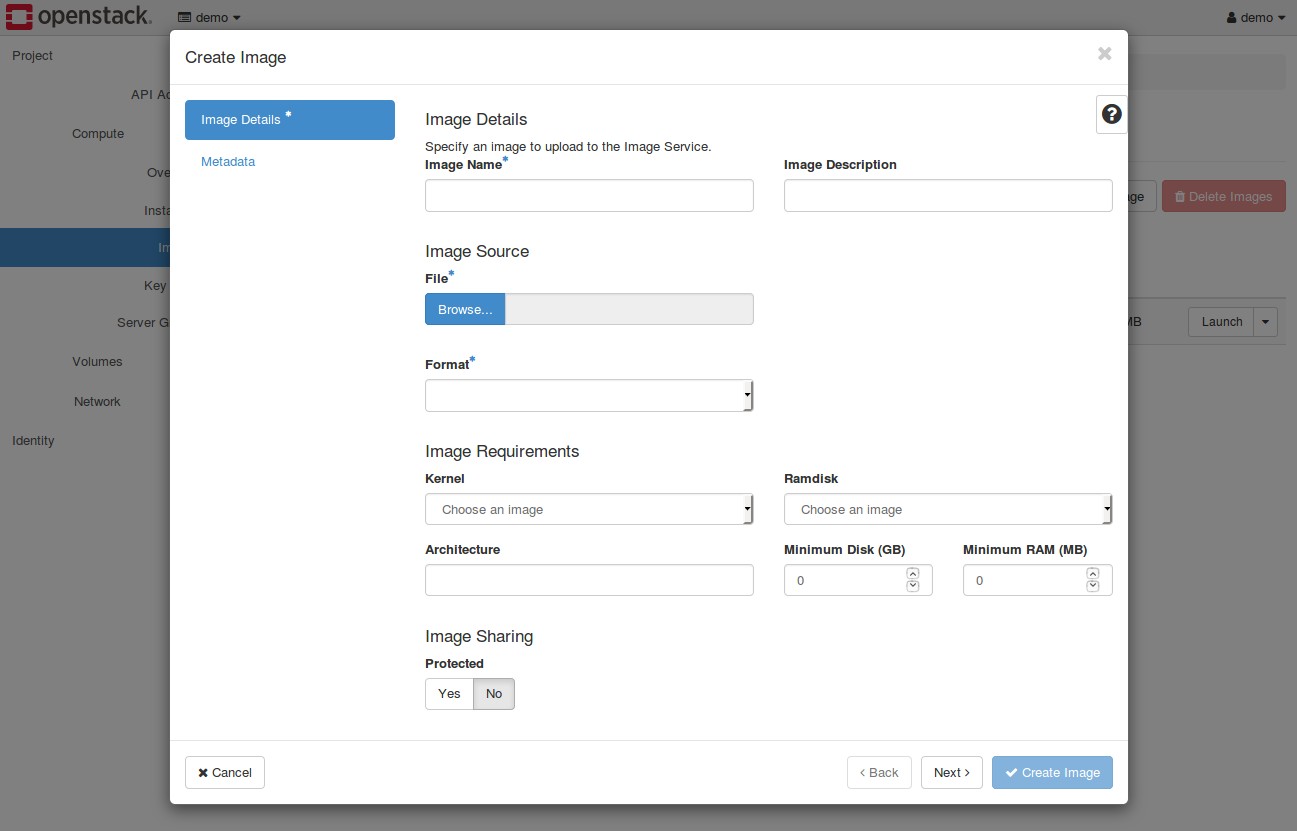
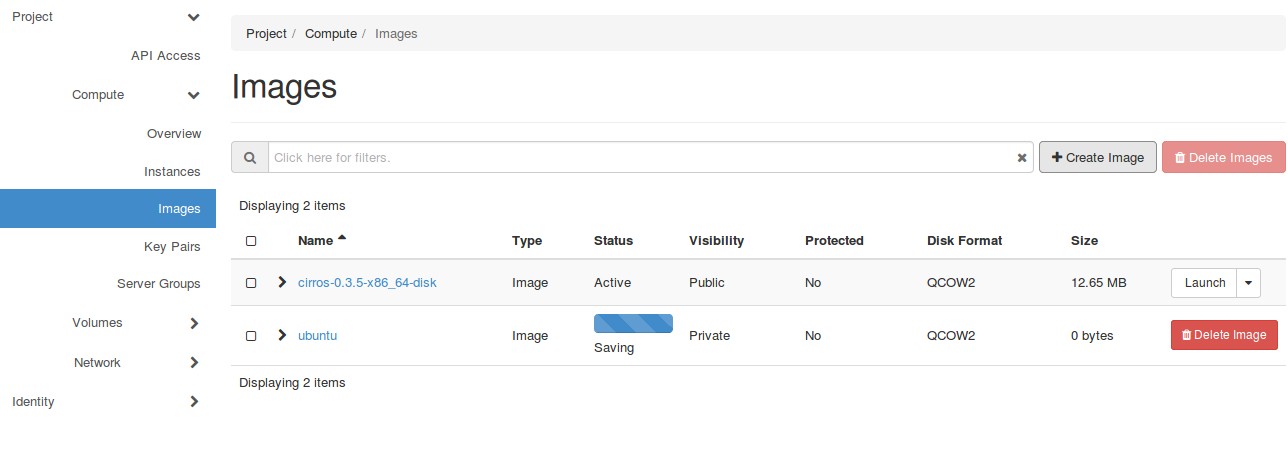


Image name: assign a name for your image.

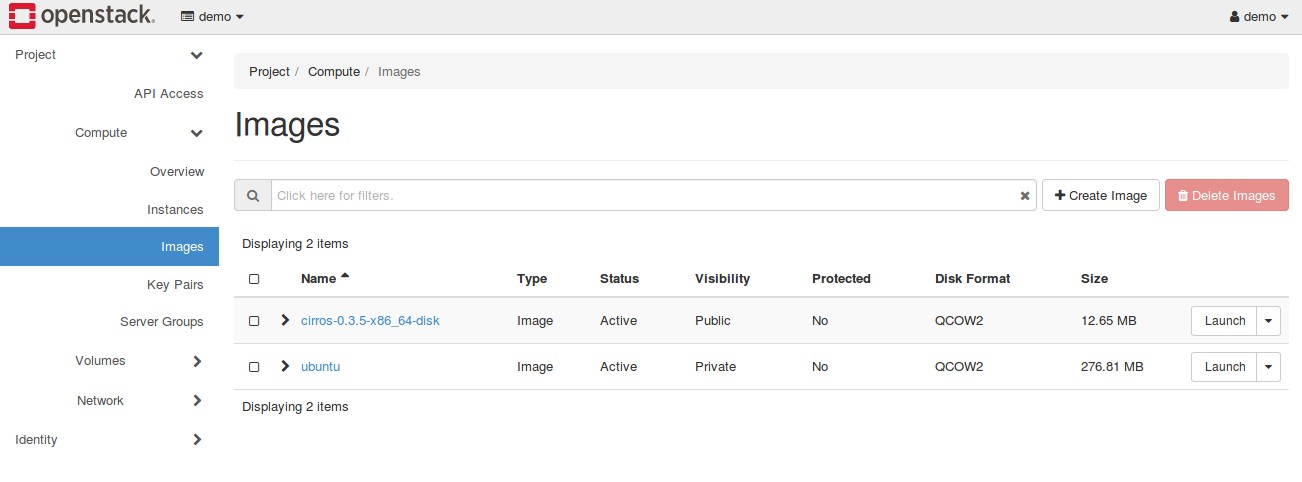
File: choose the path to the saved image file.

Format: Here we choose QCOW2 format. QCOW2 is a hosted virtual machine monitor. (Note: Please keep all other options as default. You can explore them later as good self-study.)

Now click on “create image”. Your OpenStack starts to upload and creates the image for you. Please observe the Status of the creation process.



When the uploading completes, the Status will become “Active”. If the status is still saving for more than 2 minutes, try to refresh the web page. It is worth noting that the “Visibility” of the ubuntu image is private, which means other users cannot see or use this images because you choose “no image sharing” when creating this image. This setting can be modified later. Don’t worry too much.

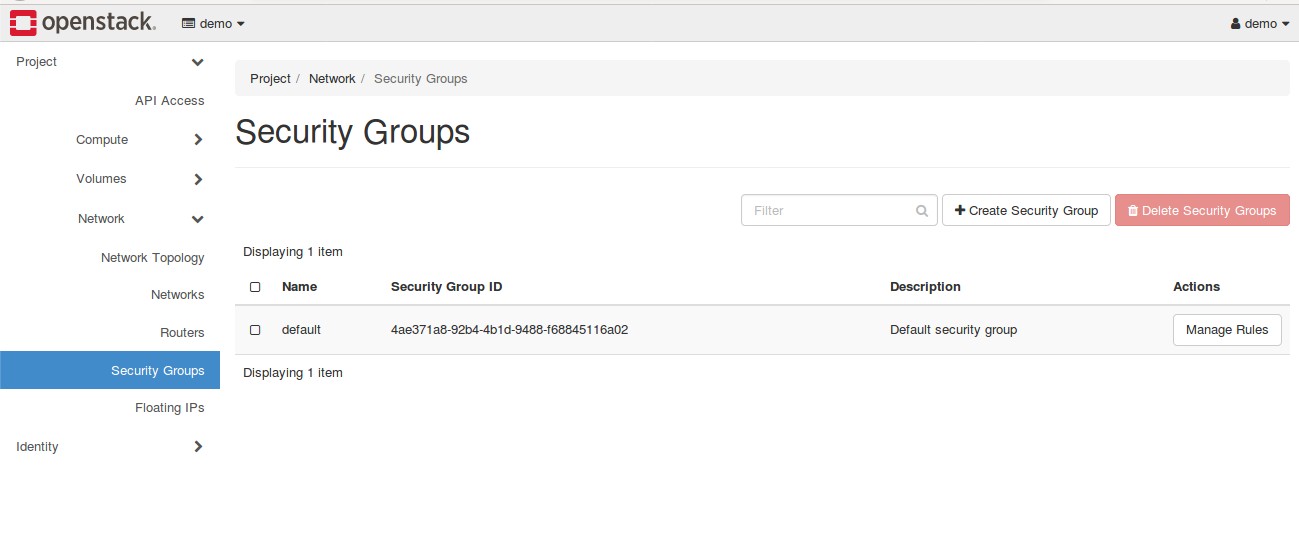


# Define a new security group

The security groups are provided in the Network service of OpenStack. A security group contains regulation rules for different network protocols supported by OpenStack networking. Allowing or disallowing the inbound and outbound data traffic can be controlled through configuring a specific security group.

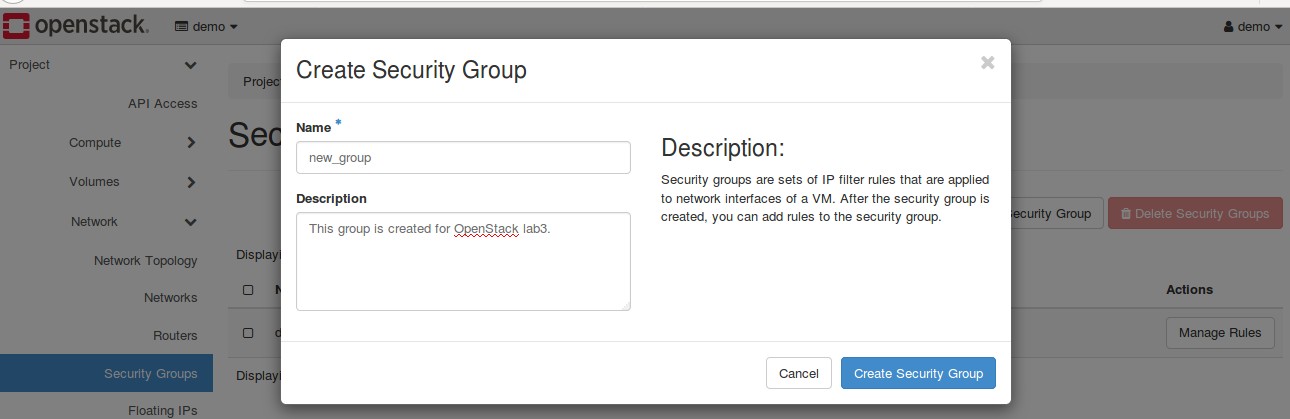
## Check you current security groups.

Now we should have only one “default” group. Click “Network” and choose “Security Groups”. Then you can click “Manage Rules” to check the exact rules in the corresponding group.



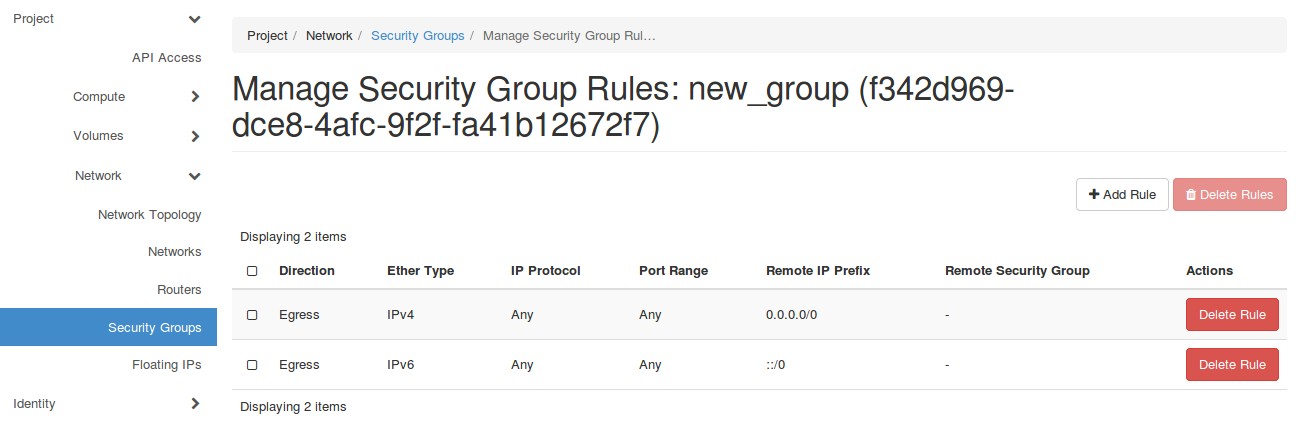
## Create your security group

Back to the “Security Groups” main page. Click “Create Security Group”. A new window will pop up and you can enter a name and add some description for the group. After that, click “Create Security Group”. On the right upside corner of the web page, a green window will appear to confirm the success of your creation.

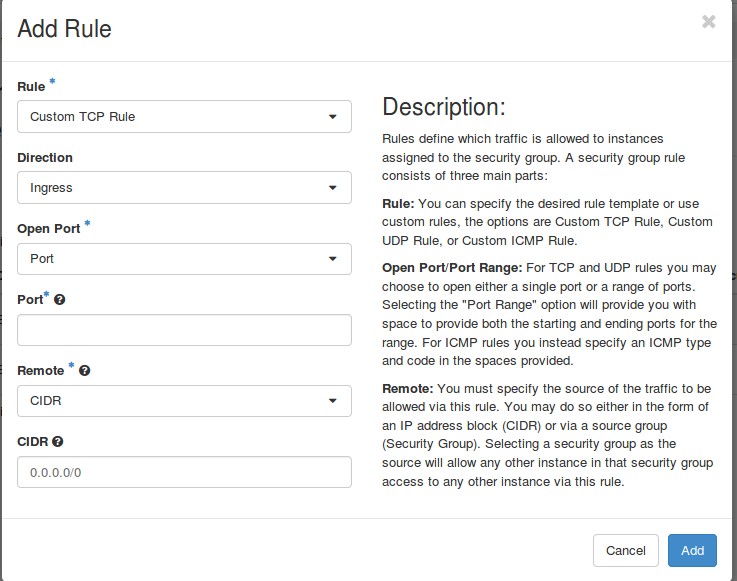


## Manage security rules

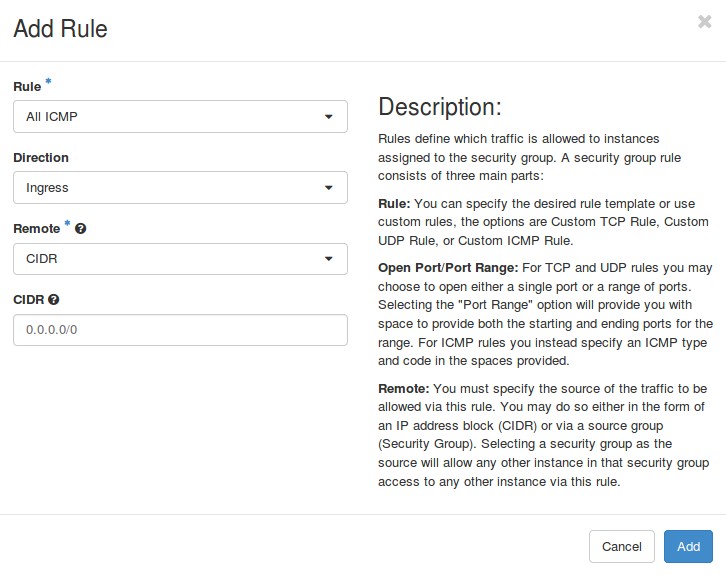
Click “Manage Rules” of the new created group. You can see the current rules. There should only exist two rules. Now we are trying to add more.



Click “Add Rule” and get a new window to configure a new rule. In the “Rule” option, we will find there are more than ten rules available. For this lab, we will use “All ICMP”, “All TCP”, “All UDP” and “SSH”.

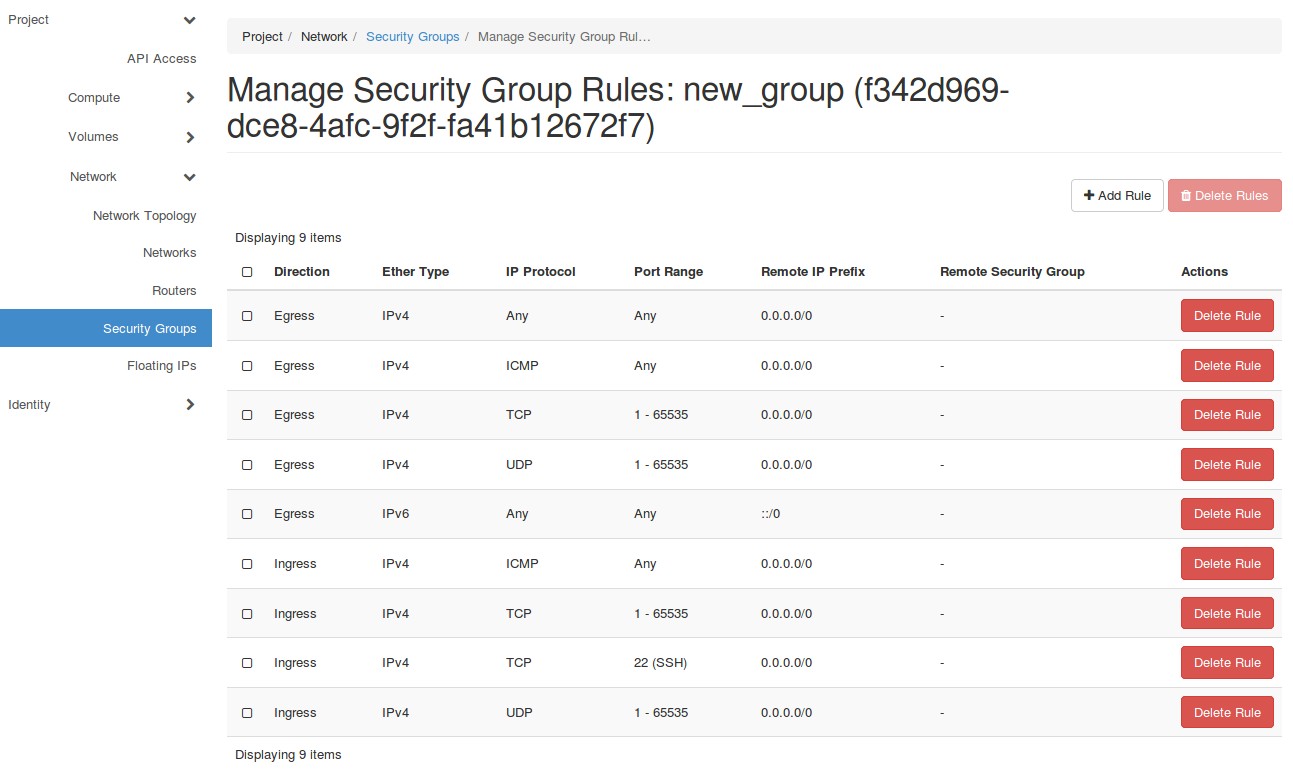


All ICMP: Please do the operating twice: one for Ingress Direction, another for Egress Direction. For your reference, an example is below:



All TCP: Do it for Ingress and Egress directions. All UDP: Do it for Ingress and Egress directions. SSH: No direction option. Simply add SSH protocol.

Now you get a ready-to-use security group like the below. This new group allows us to make a ping test to an instance and remotely access it.

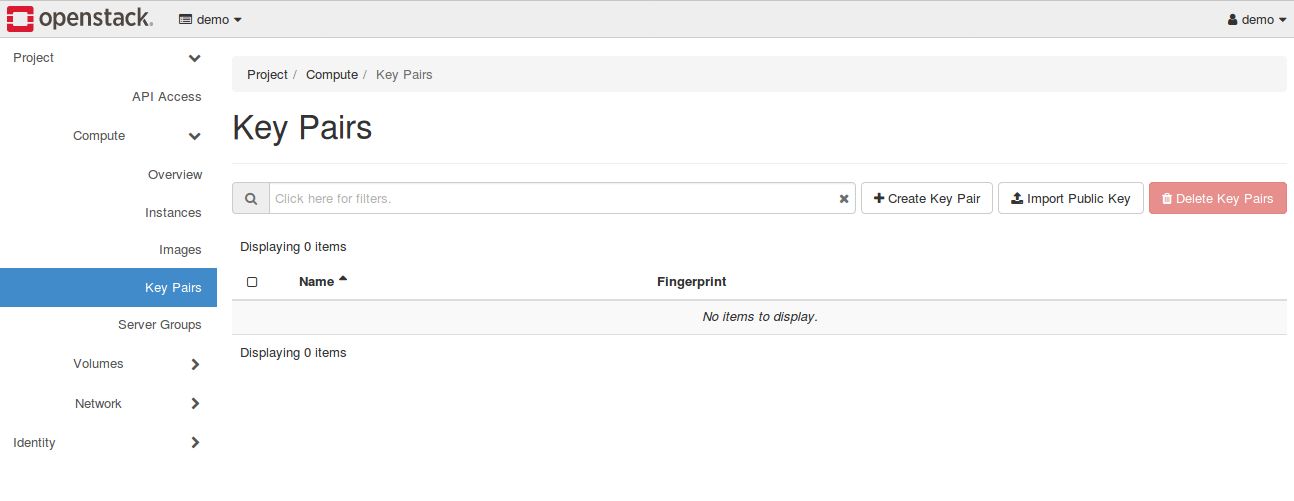


# Create key pairs

A key pair allows us to remotely access to the Ubuntu instance using SSH because Ubuntu does not have username and password to log in directly through web console.

## Check your key pairs.

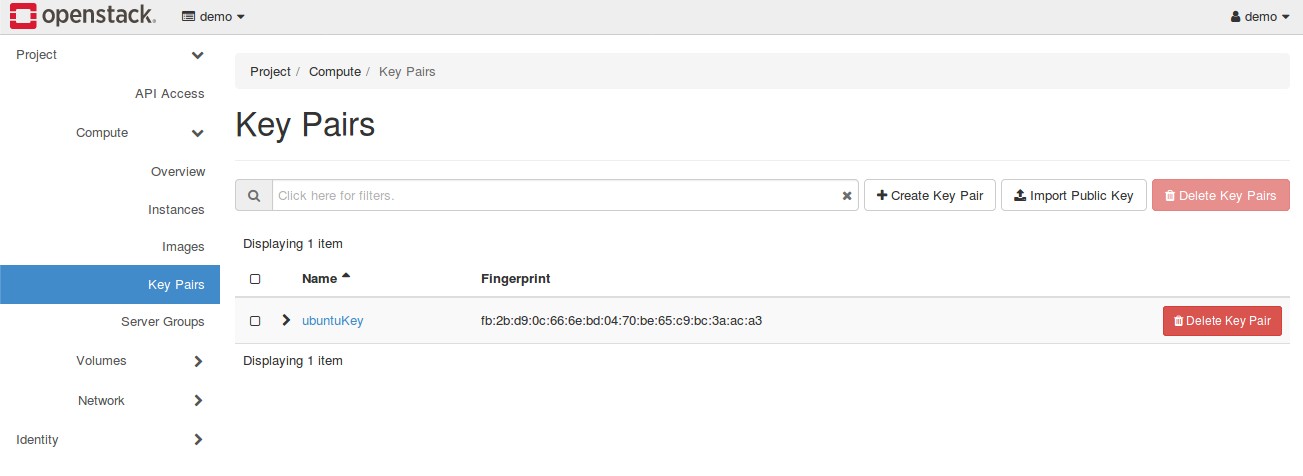
In the “Compute” section, click “Key Pairs”. Your current keys will be listed. Now we have no keys.



## Create a new key pairs.

Click “Create Key Pair”. You only need to give a name. A new key will be generated and you are asked to save a key in your local machine. Please save it to a safe place since you will use it to access you instance later.

Now you already have a new key. The key downloaded is the private key so it can only be available when you create it. There is no other way to obtain it again. Be careful! The public key is uploaded to the OpenStack automatically where Keystone service manage it for you.

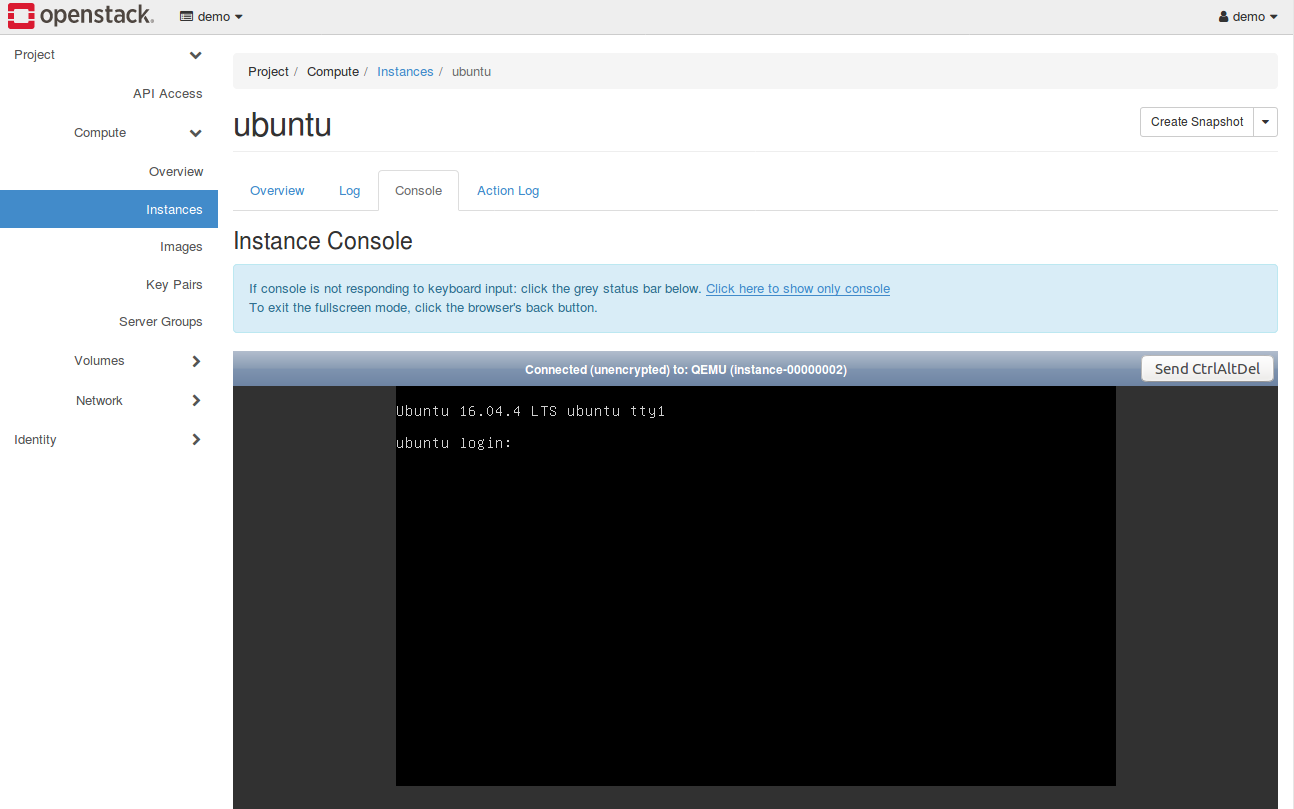


# Launch and SSH Ubuntu instance

Now we can launch an Ubuntu instance under the configurations of our new security group and key pair.

## Launch instance

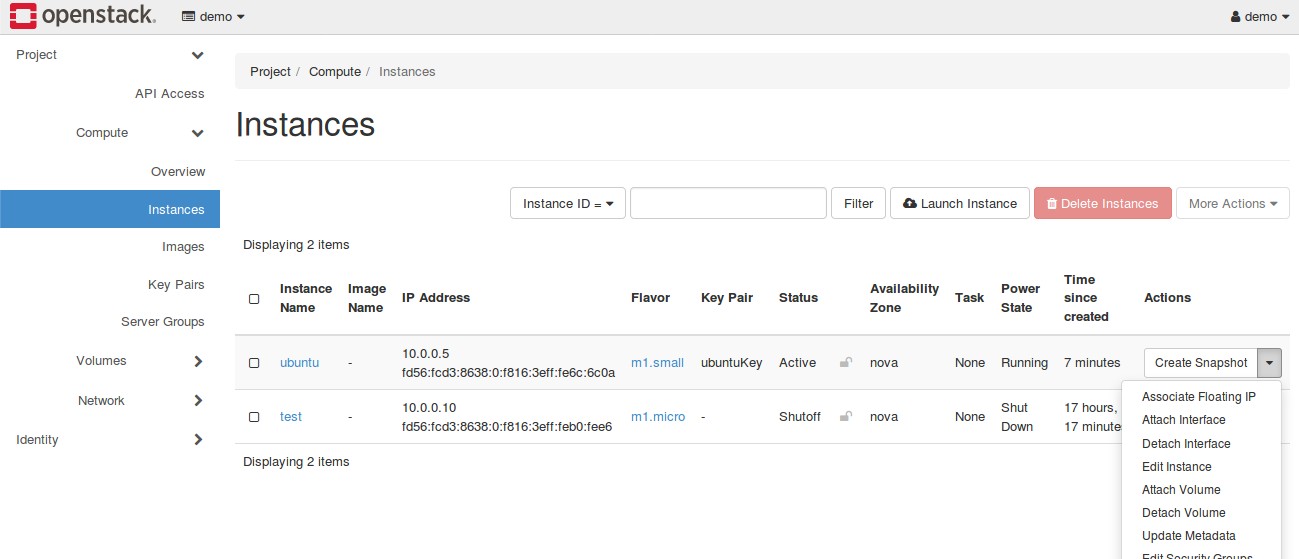
The steps to launch an instance are same as steps in Lab 2. Remember to choose ubuntu image, use a bigger flavor (like ds1G or m1.small), pick the ubuntu security group and allocate the key pair. You may need to wait several minutes for booting the instance. Please observe the “Log” and “Console” during the spawning process. When the instance is ready, you will see the following message:



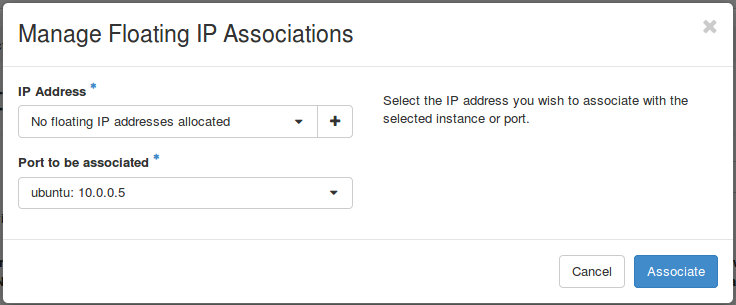
## Associate floating IP

The new instance needs a floating ip to be accessed from external network. Remember, you machine running OpenStack is on the public network but the instance is on the virtual network. The floating IP assign a public address to it.

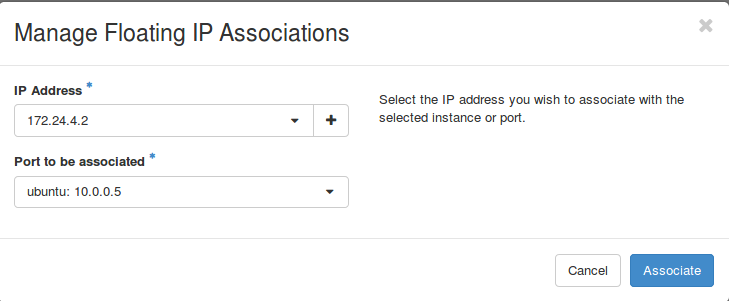
Click the drop-down box “Action” of the Ubuntu instance, and choose “Associate Floating IP”.



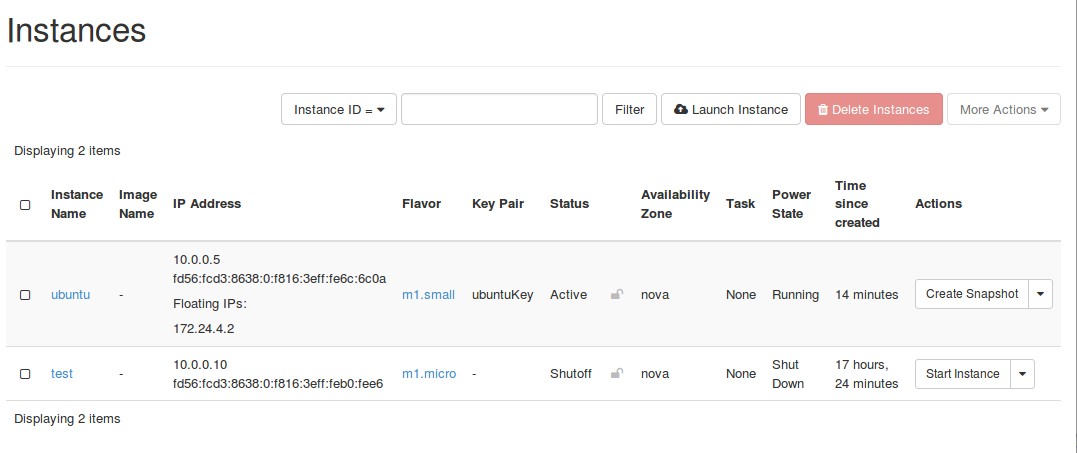
In the pop-up window, you should add a new floating IP because of no available IPs. Next, just click “Allocate IP”.



Now you have a new floating IP. Choose and associate it to your instance. Click “Associate” to finish it.



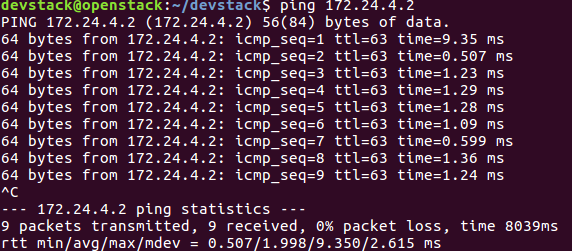
In the “Instances” page, you can find the information of the Ubuntu instance is updated with a floating IP.



## SSH the instance

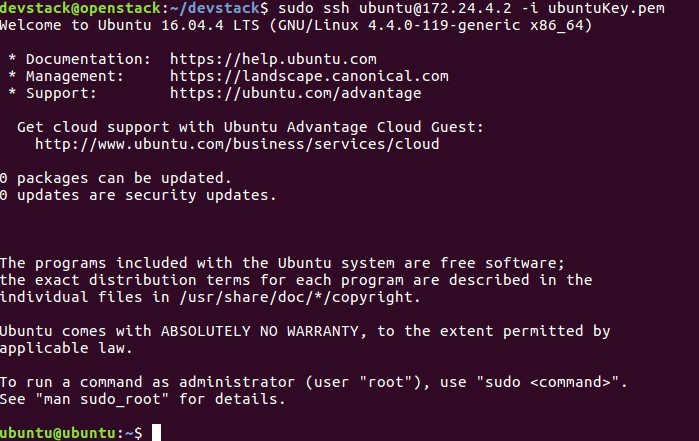
First, let’s test the ICMP protocol. Open a terminal on your local machine and enter:

$ ping Your\_Floating\_IP



Then, change the directory to the folder which saves the private key and enter:

$ sudo ssh ubuntu@Your\_Floating\_IP ­i PrivateKeyName.pem



Now you have already logged in the Ubuntu instance. You can operate it like a new computer. Have fun and enjoy your success!

# What to Hand in

1. Please make a screen shot for the rules of your new security group.
2. Submit the Logs you observe during the launching of the Ubuntu instance.
3. Please create a new folder after you ssh to Ubuntu. Name the folder with “Your Name\_Lab3”.
4. Report the private IP and the floating IP associated with your Ubuntu instance.