User recommendations to secure virtual machines in OpenStack

Securing access to the Virtual Machine

One of the easiest ways for an advisory to get access to a virtual machine in the cloud is through poorly configured login credentials. there are bots on the web that will try to brute force login username and passwords on exposed ssh interfaces. It is therefore important for all machines to use strong login methods. One of these methods is to use a public private key pair instead of a password. Bellow are the instrustions on how to set up an ssh keypair.

1. Ensure that one has created an ssh key pair.

- In a terminal run the following command:

```
$ ssh-keygen -t rsa -b 4096
# The `ssh-keygen` command will create the key
# The `-t` option will set the cryptosystem to rsa
# The `-b` will set the key length to 4096 bits
Generating public/private rsa key pair.
Enter file in which to save the key (/home/groot/.ssh/id_
rsa) #Your path goes here
```

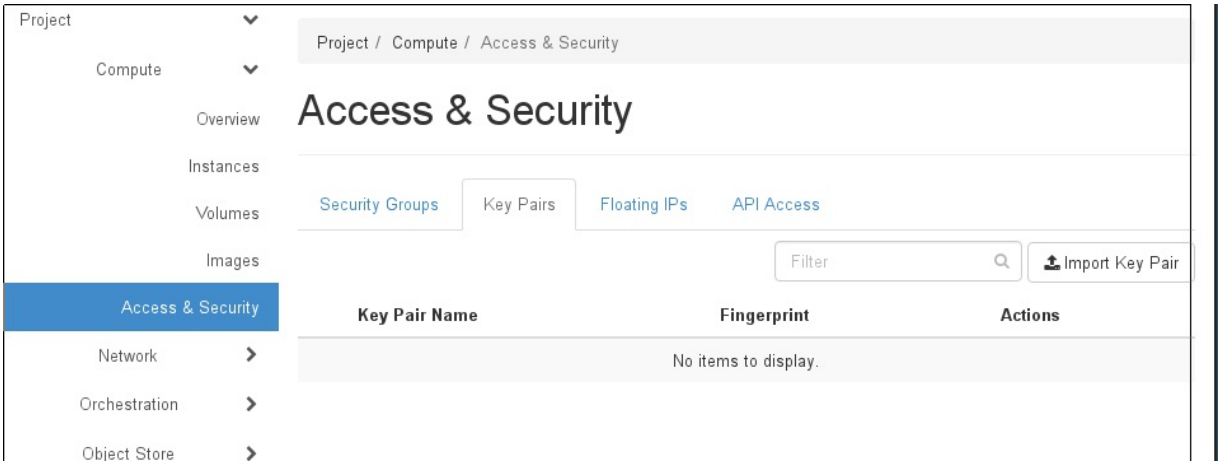
```
Enter passphrase (empty for no passphrase) #Enter a passw
ord
Enter same passphrase again: #Reenter your password
...
```

- You now will have a public and private key pair in the location that you specified. You can then submit your public key (`.pub`) when you try and `ssh` into a machine.

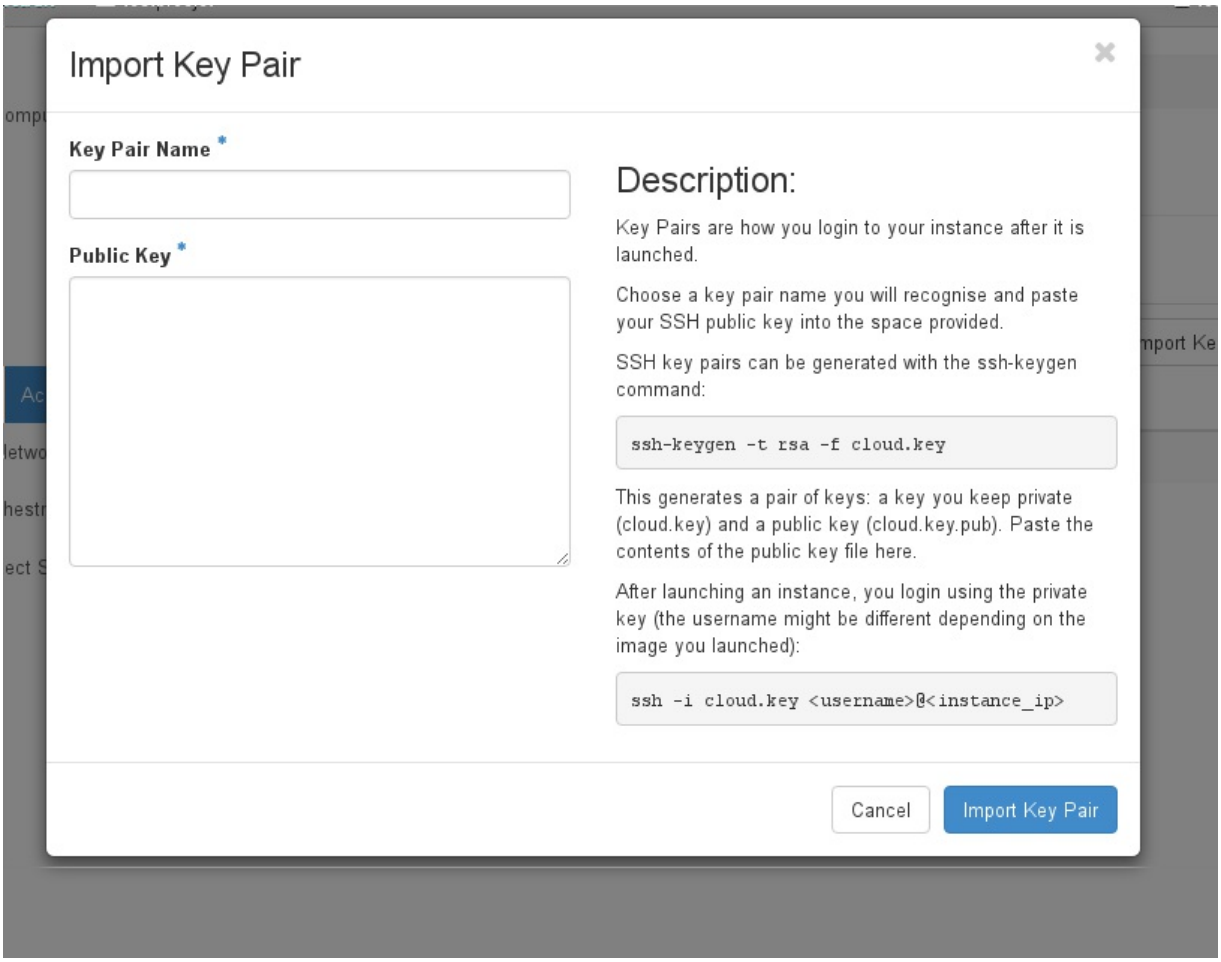
```
$ ssh -i #Path to your private key# username@machine
```

2. You must upload your public key into OpenStack control panel:

- Login to the OpenStack administration panel and select “Access & Security” in the left hand column.
- Next select the “key Pair” located to bellow the “Access & Security” title.



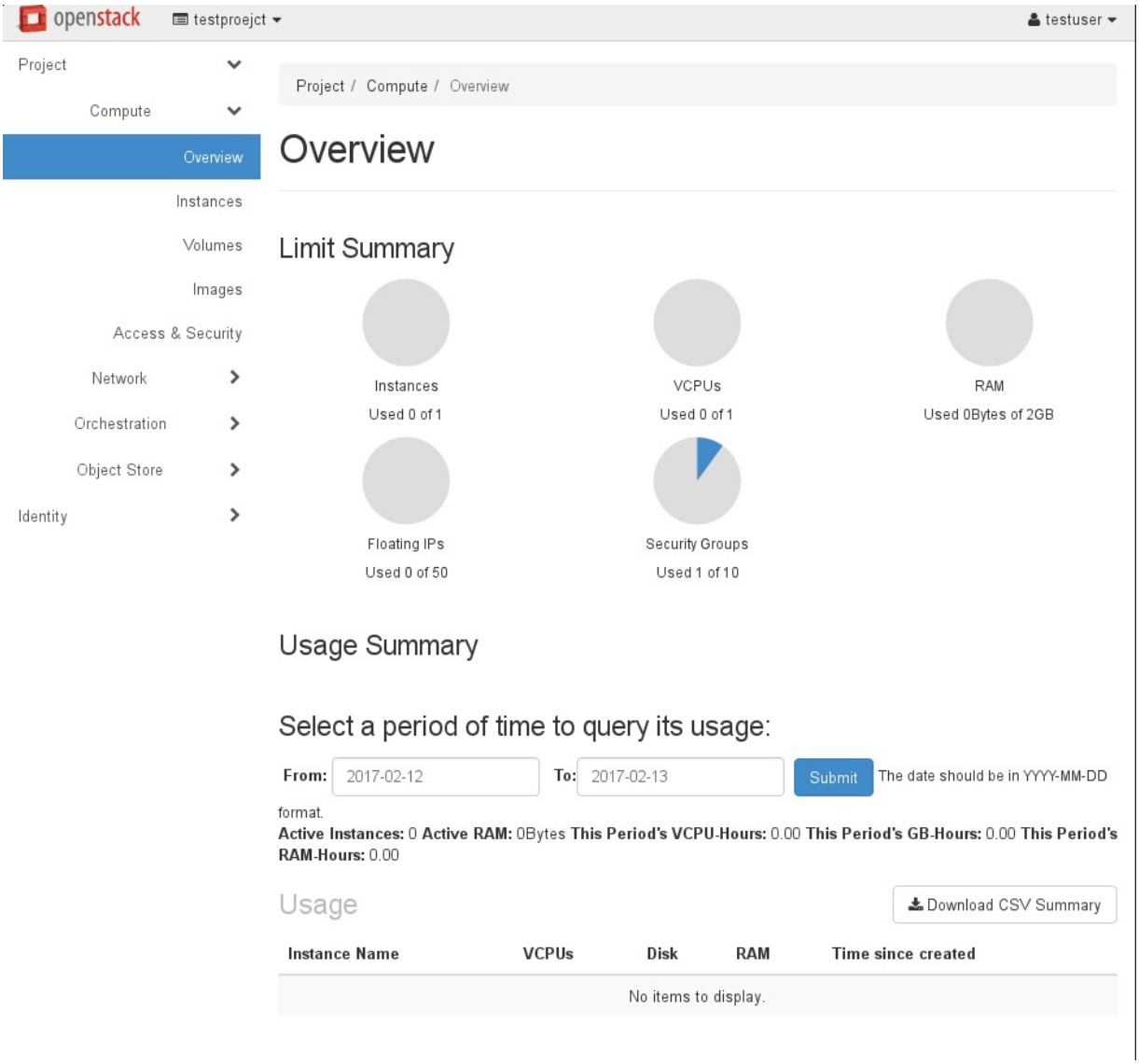
- Once on the page proceed to click on the “Import Key Pair” button located at the top right of the screen.
- A pop-up should appear that looks similar to the following:



- Go back to your terminal and find your public key (`.pub`). Copy the contents and paste them into the field marked “Public Key”. Then add a name to your key and click the “Import Key Pair” button at the bottom of the pop-up.

Creating a new machine

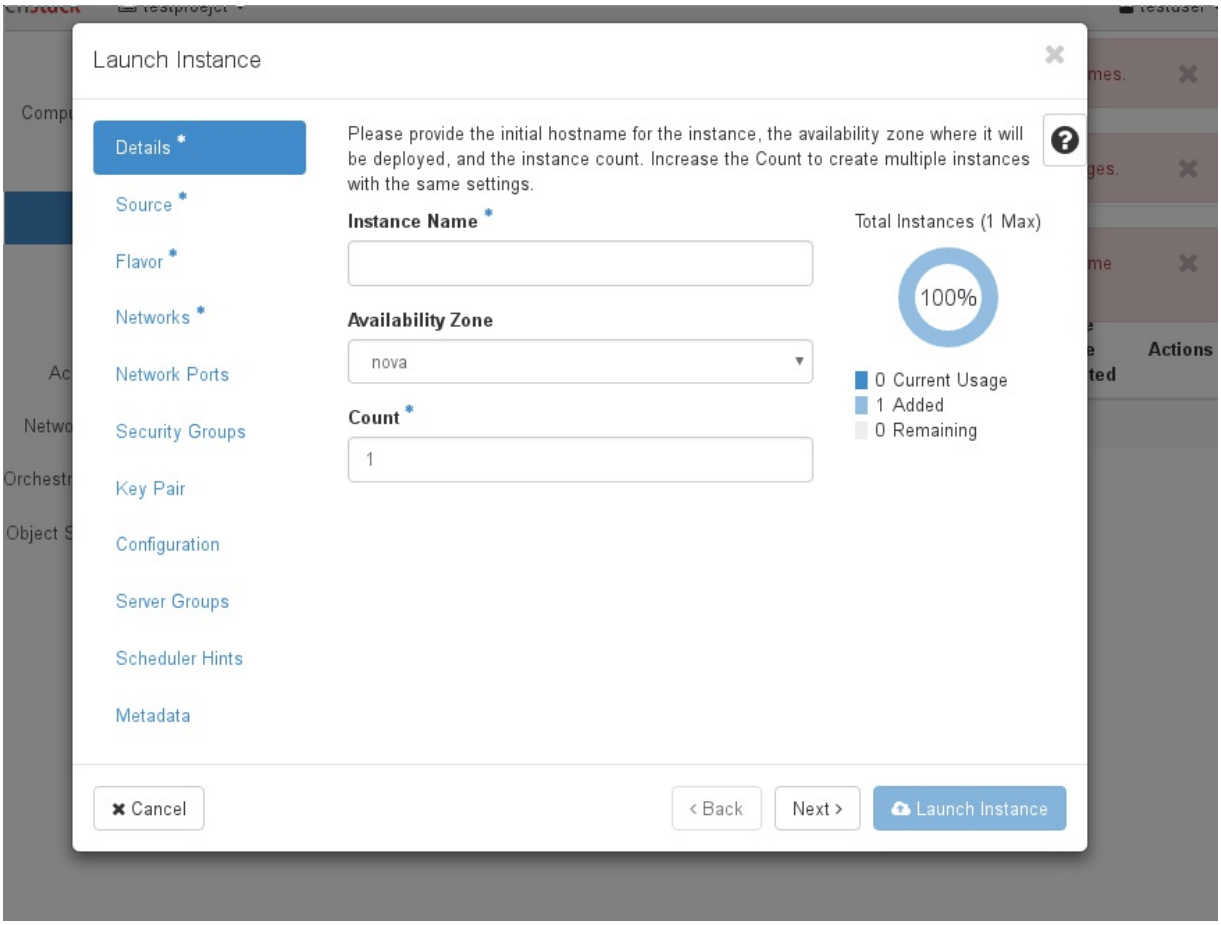
1. Access the main control panel for OpenStack:



2. Select the “Instance” tab on the left hand side of the screen.

3. Now select the “Launch Instance” button on the upper right hand side of the screen.

4. A pop-up should appear that look similar to the following:



5. Fill out the necessary setting.

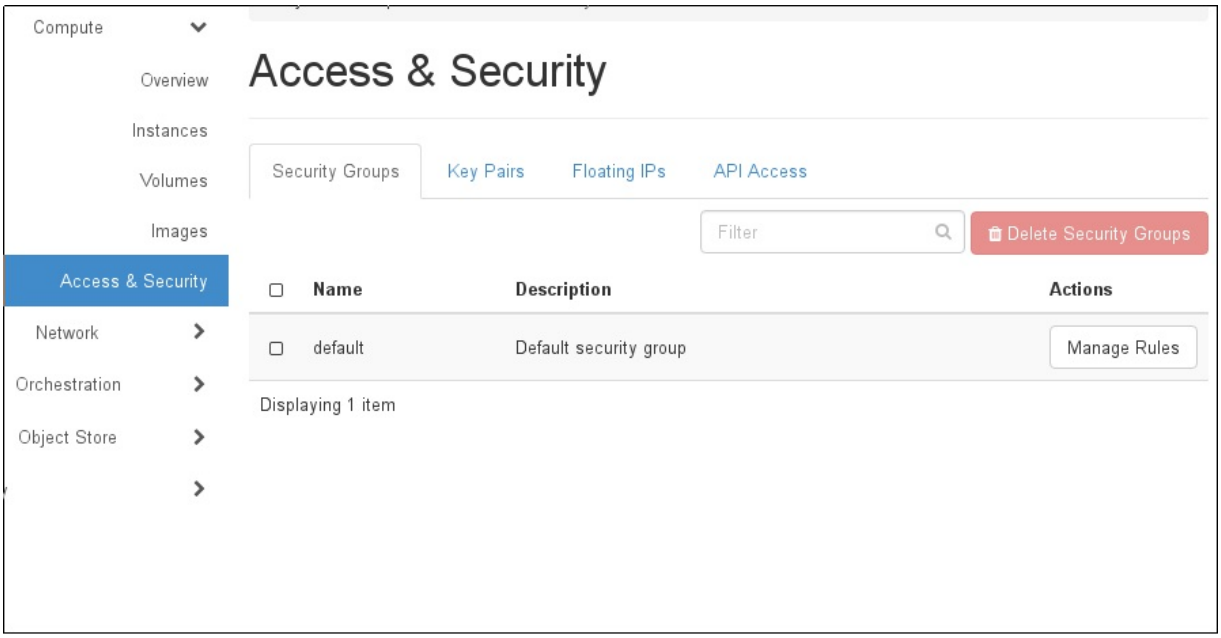
- Ensure that the “Security Group” tab has the correct group assigned to the VM.
- Ensure that the correct public key is selected in the “Key Pair” tab

Security Rules

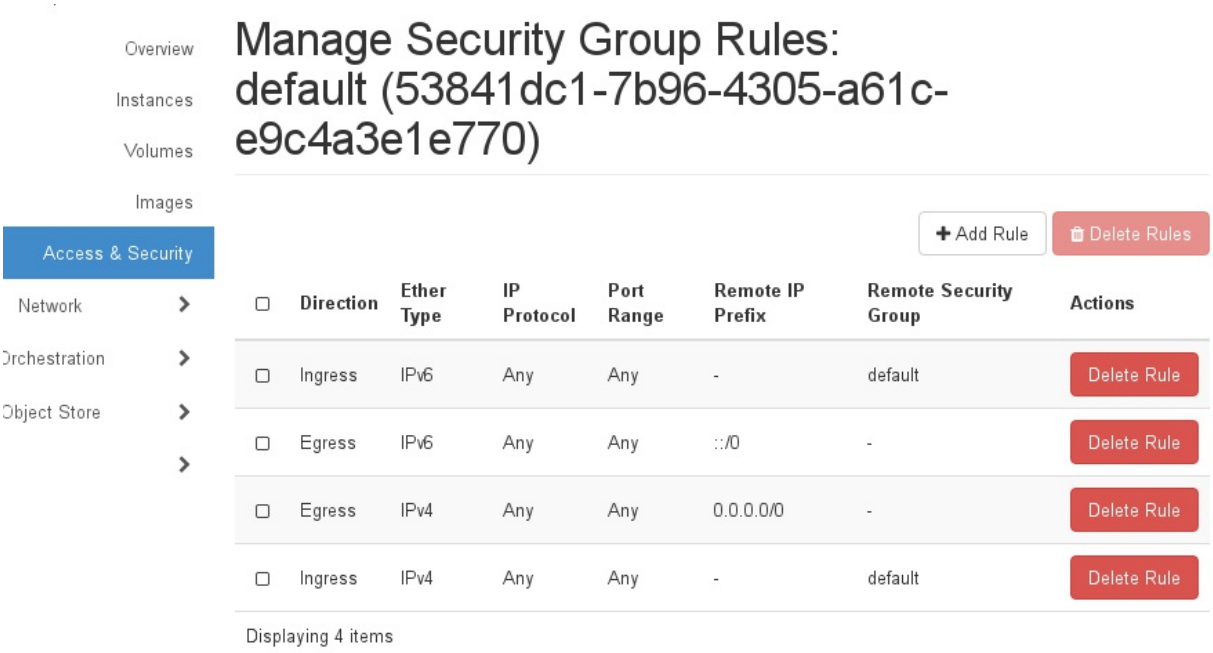
Security rules are a set of instructions that can be placed on to VMs that will limit that particular VMs ability to access external environments. They act very similar to a firewall with allowing or blocking different types of connections to the individual VMs. To set up proper rules the following steps should be taken:

1. Log into OpenStack and select the “Access & Security” tab on the left hand side.

2. You will now see a list of security groups that you are part of. Select the group that you would like to edit by clicking the “Manage Rules” button on the right hand side.



3. The new screen should look something like this:



Lets break down what the different components are:

- The “Direction” field describes if inbound or outbound traffic is affected by the rule
- “Ether Type” describes wether the rule talks about IPv4 or IPv6 traffic
- “IP Protocol” describes what type of traffic is permitted or blocked (i.e. http, pop3, etc.)
- “Port Range” what ports that rule applies to for that machine
- “Remote IP Prefix” describes what IP address the traffic should come from

As with any computer system accessible to the internet great lengths should be taken to ensure that a machine can not be compromised. As

cloud based solutions often see machines turning on and off frequently a strong set of “Security Rules” can help ensure a healthy virtual environment. Bellow are a set of recommendations to follow:

- Only allow port 22 (ssh) and only the ssh protocol to be allowed to connect to VMs from remote hosts.
- If a machine or group of machine dont need access the the internet (i.e. database machine) ensure that the security group only allows internal network traffic to come from and to that machine.
- Open only the necessary port for specific machines to access the internet.
- If feasible block all outgoing traffic (ensure that one does not block ssh if needed to connect from the outside) and then open only the ports that are needed.

A good reference point for security rules are Linux iptable rules (http://netfilter.org/).