How to setup Computer Canada Cloud to run ONOS

About Computer Canada Cloud

Because the DICES apps requires ONOS system and Mininet, the project cannot be completed using only localhost resources.

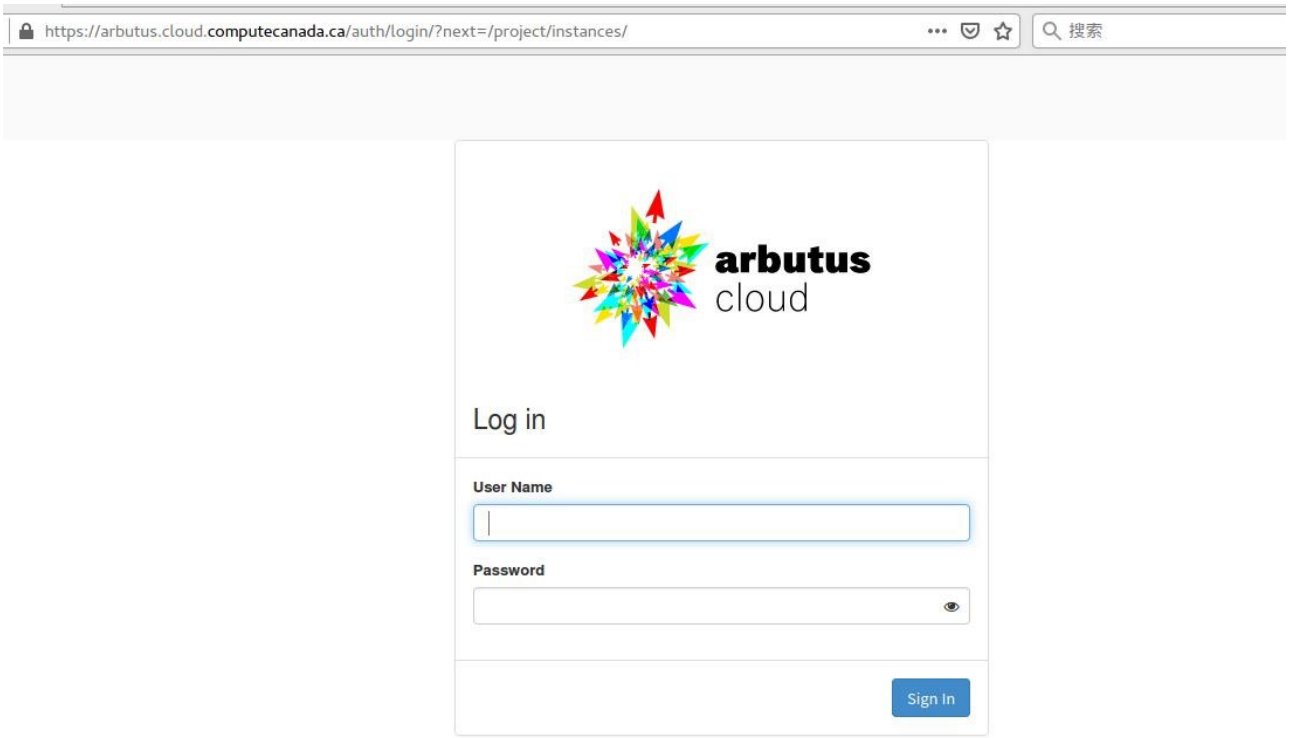
The Compute Canada Cloud service can provide researchers who require greater configurability, availability, durability clusters. Meanwhile, the cloud can provide researchers with virtual machines to meet their personal needs, including setting the size of RAM, setting the size of hard disk, setting the number of CPU cores, and the version and the Linux system version. It also provides root permission so that it meets the requirements of running DICES with ONOS and Mininet.

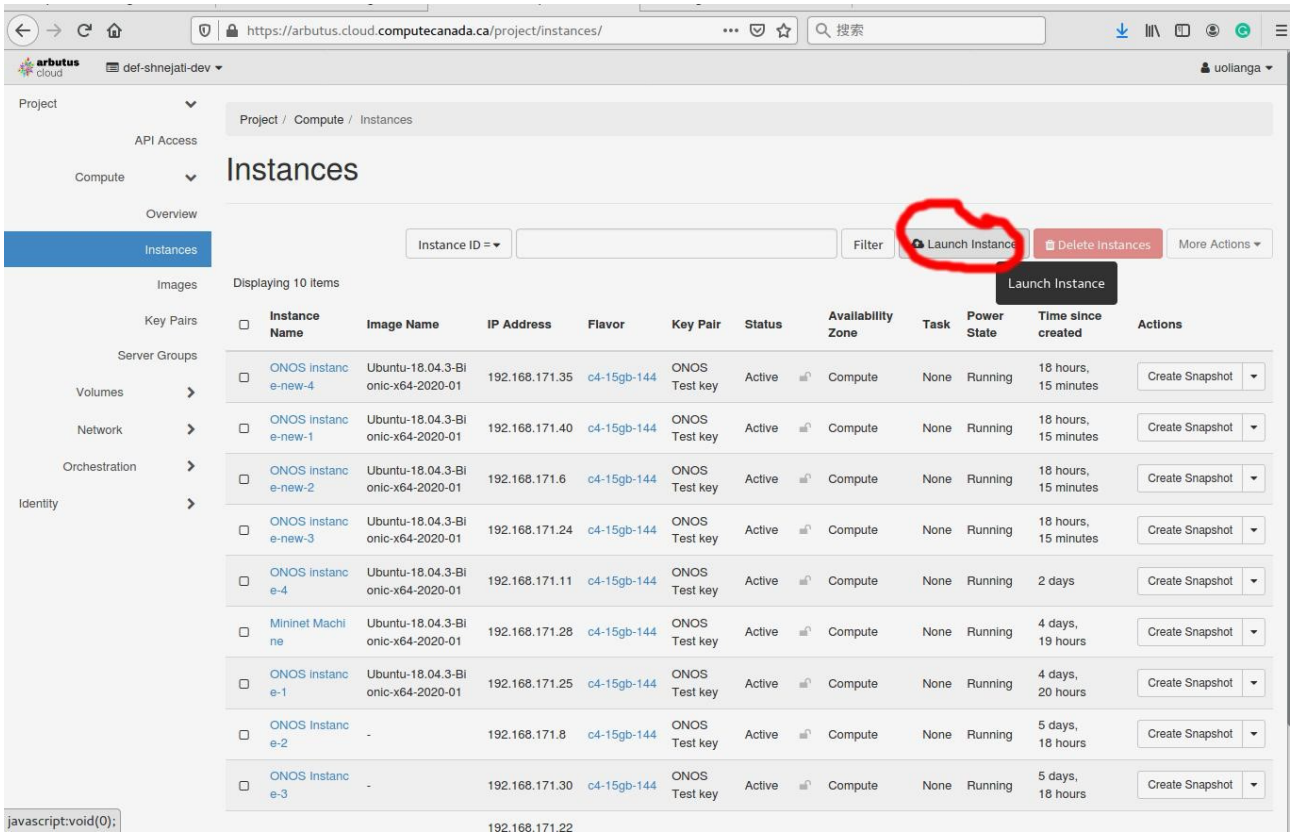
Firstly, let us try to create an instance on CCC (Compute Canada Cloud).

The ONOS version in this project is *ONOS-1.15.0*.

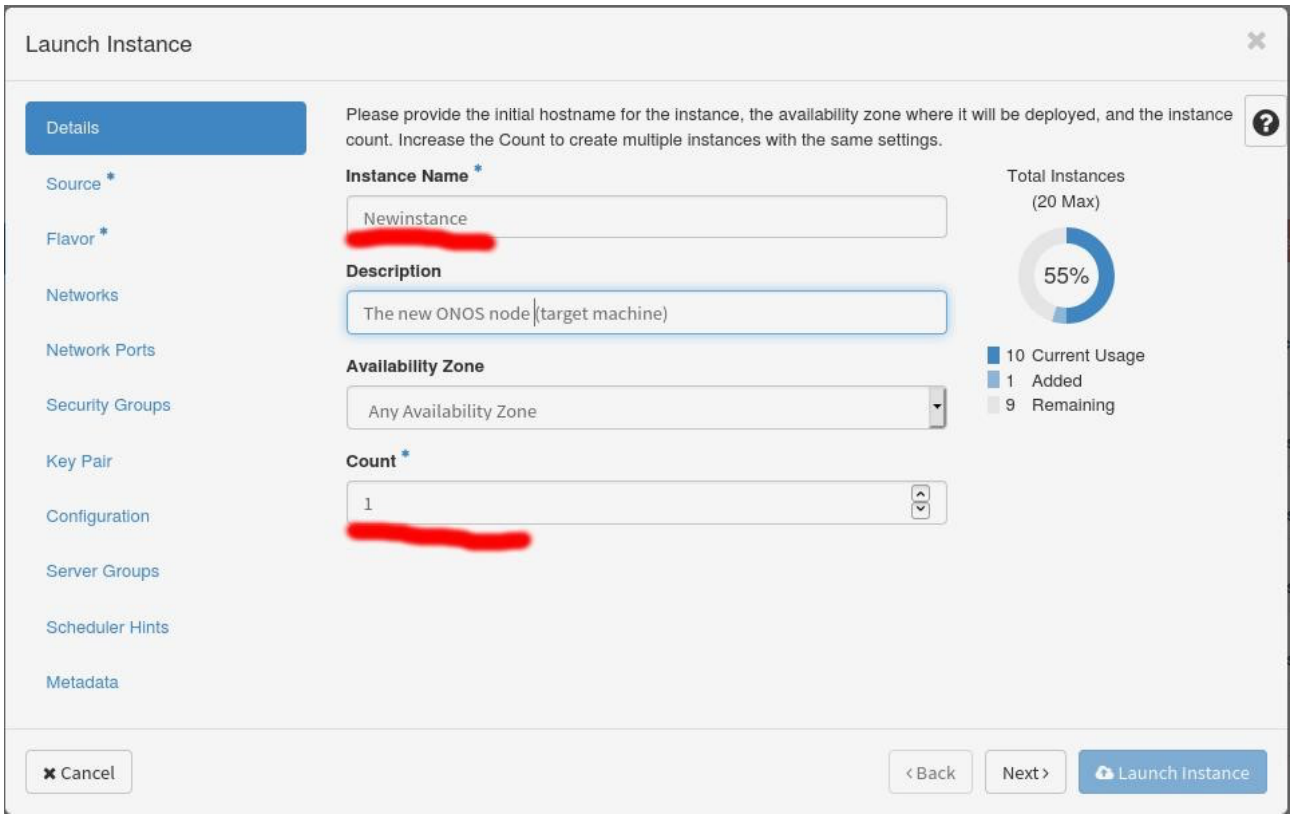
Now let us create the machines first:

Go to *https://arbutus.cloud.computecanada.ca/auth/login/?next=/project/instances/* and login to the account.

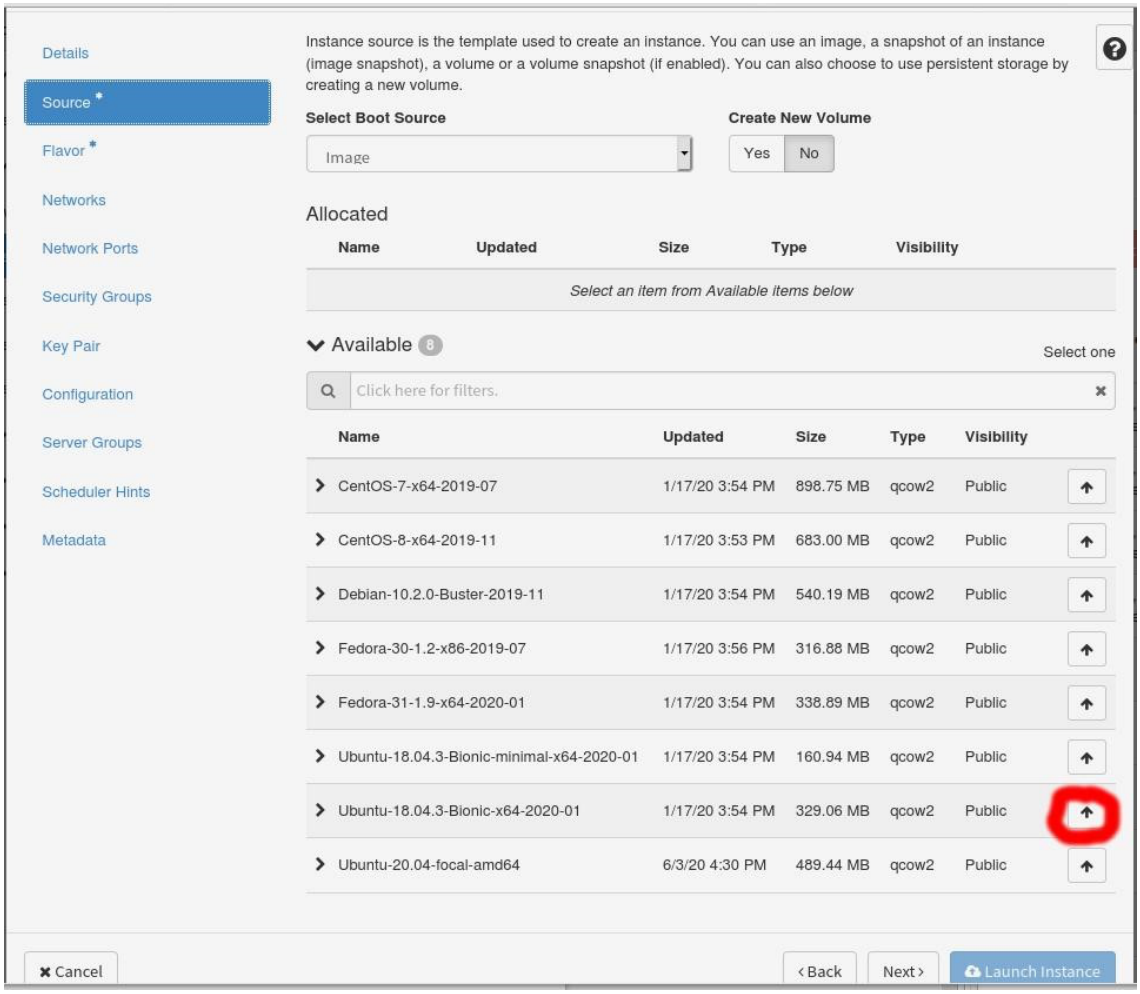




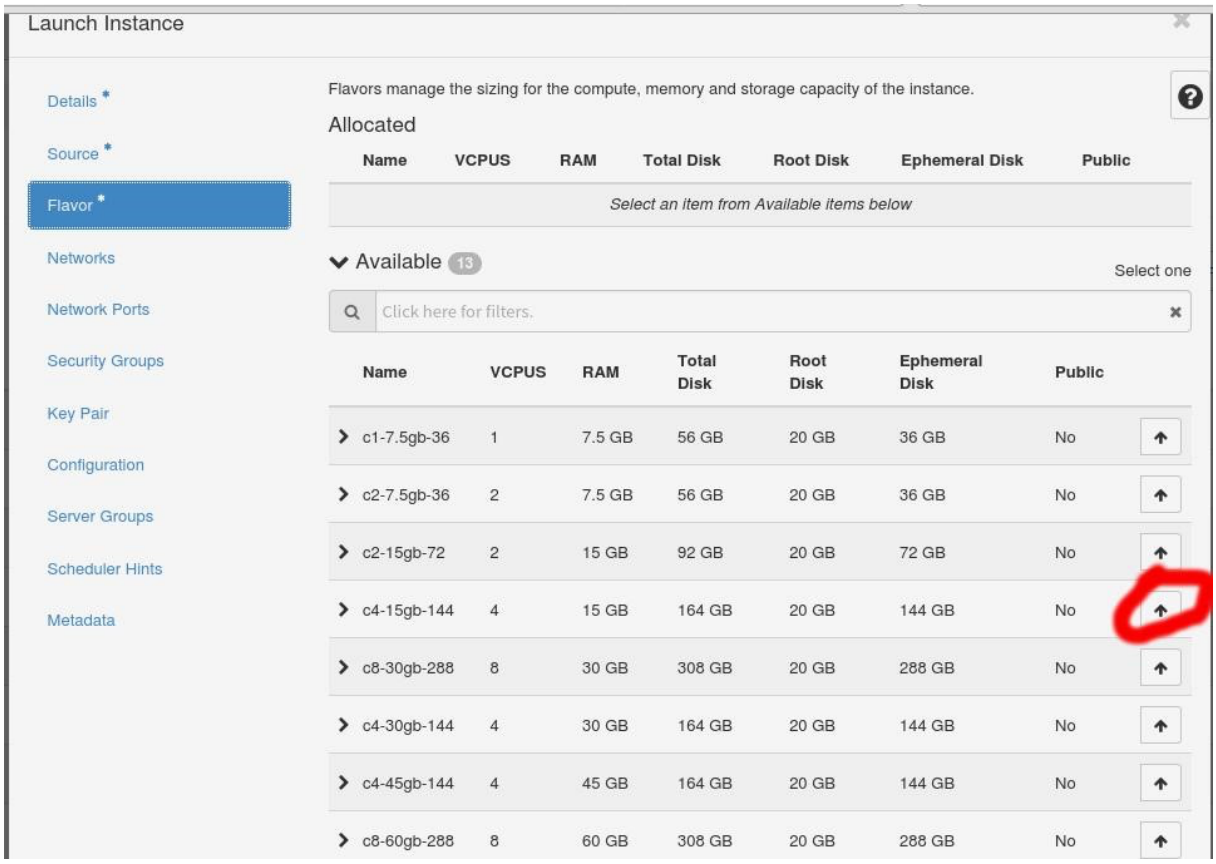
And then let us go to *Instance* tab and click *Launch Instance* button.



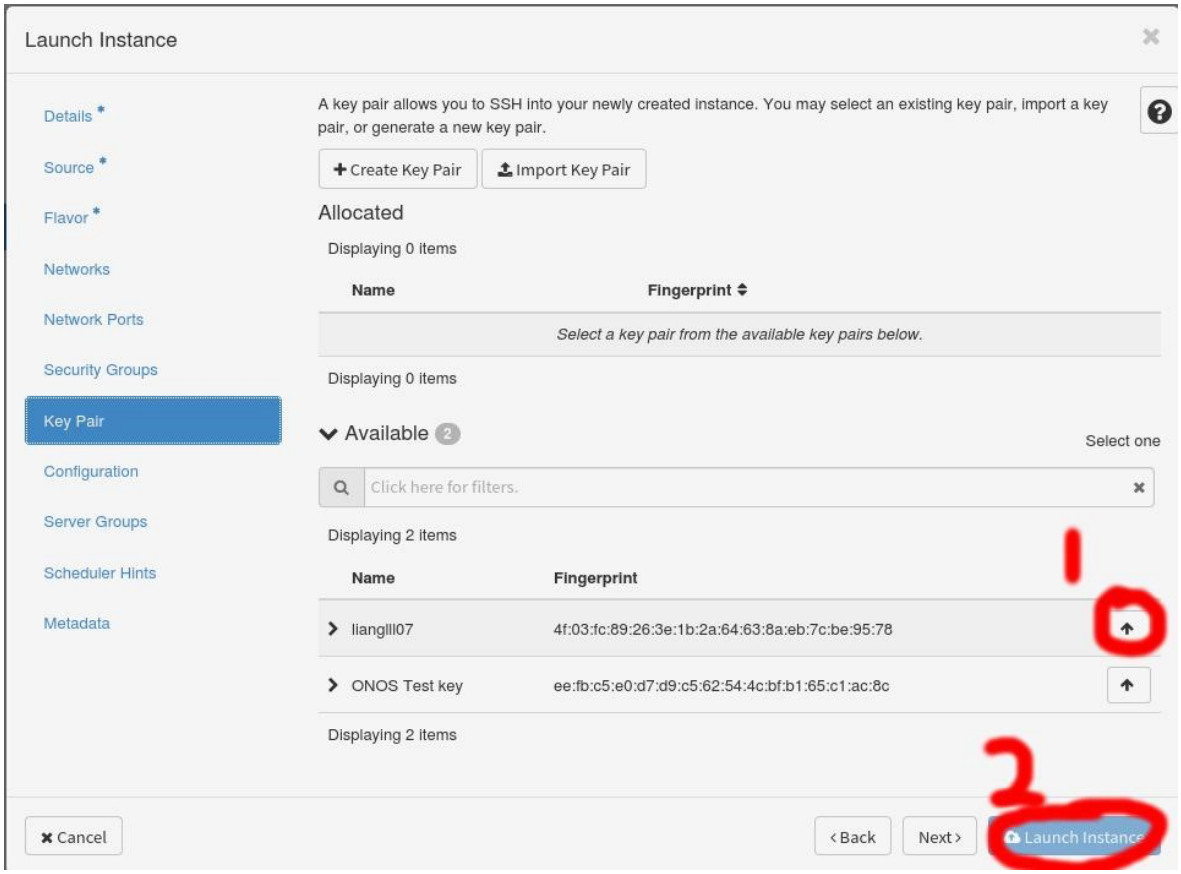
Then in the *Detail* tab, enter *Instance Name* and *Count* (The number of the instance you want to create). You can also enter the *Description* of the instance if you need.



Then in the *Source* tab, choose the image to build up the machine. For this project, we use Ubuntu-18.04. Click the “Up” button as shown.



Then in the *Flavor* tab, choose the following one which is meet test requirements. Of course, we can also choose a higher configuration, but the overall resources are limited. It depends on the user.



Finally, in the *Key Pair* tab. I have already created one key so just click the “Up” button and then we can launch our instance.

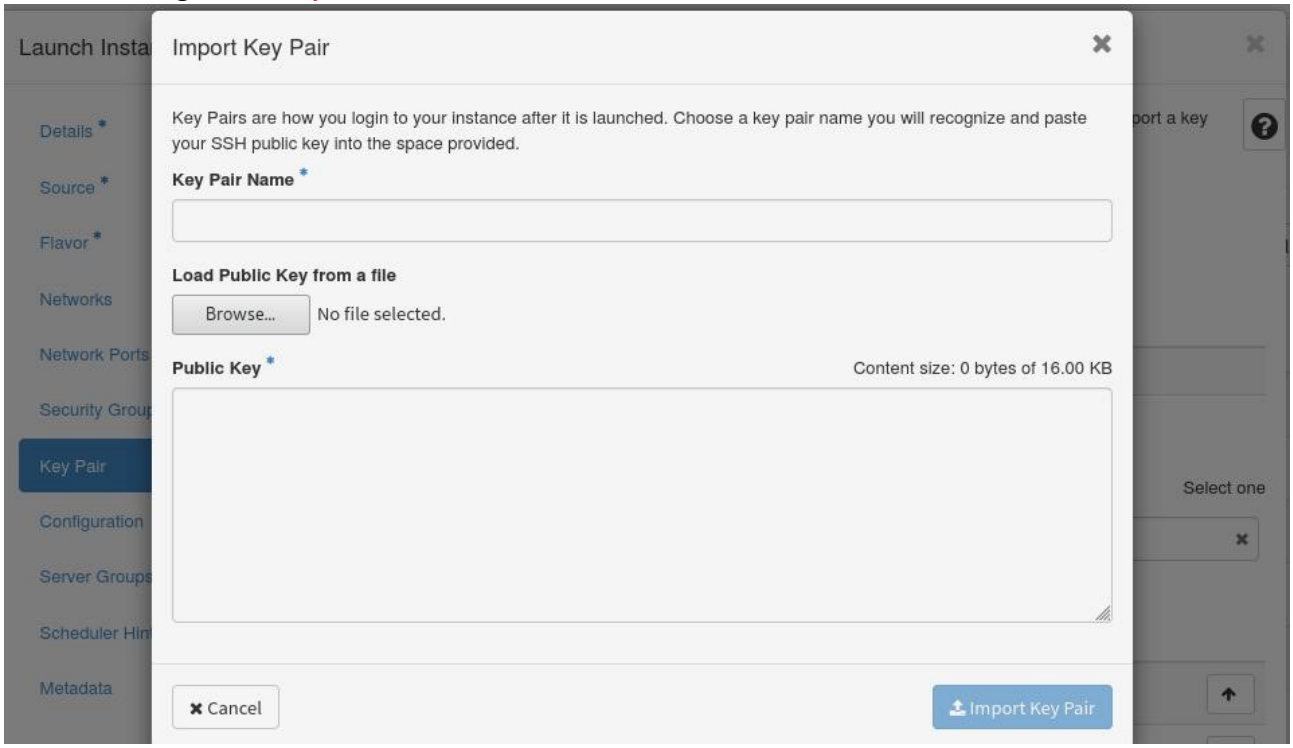
Optional:

In addition, if you want to use a new key pair. In your computer, open a terminal and enter:

ssh-keygen -t rsa

(**For convenience, please do not set the password here**)

It will generate an *id_rsa* (**private key**), *id_rsa.pub* (**public key**) and *authorized_keys* in ~/.ssh folder
Then click *Import Key Pair* as shown above and then copy your public key in ~/.ssh/id_rsa.pub to the following *Public Key* blank:



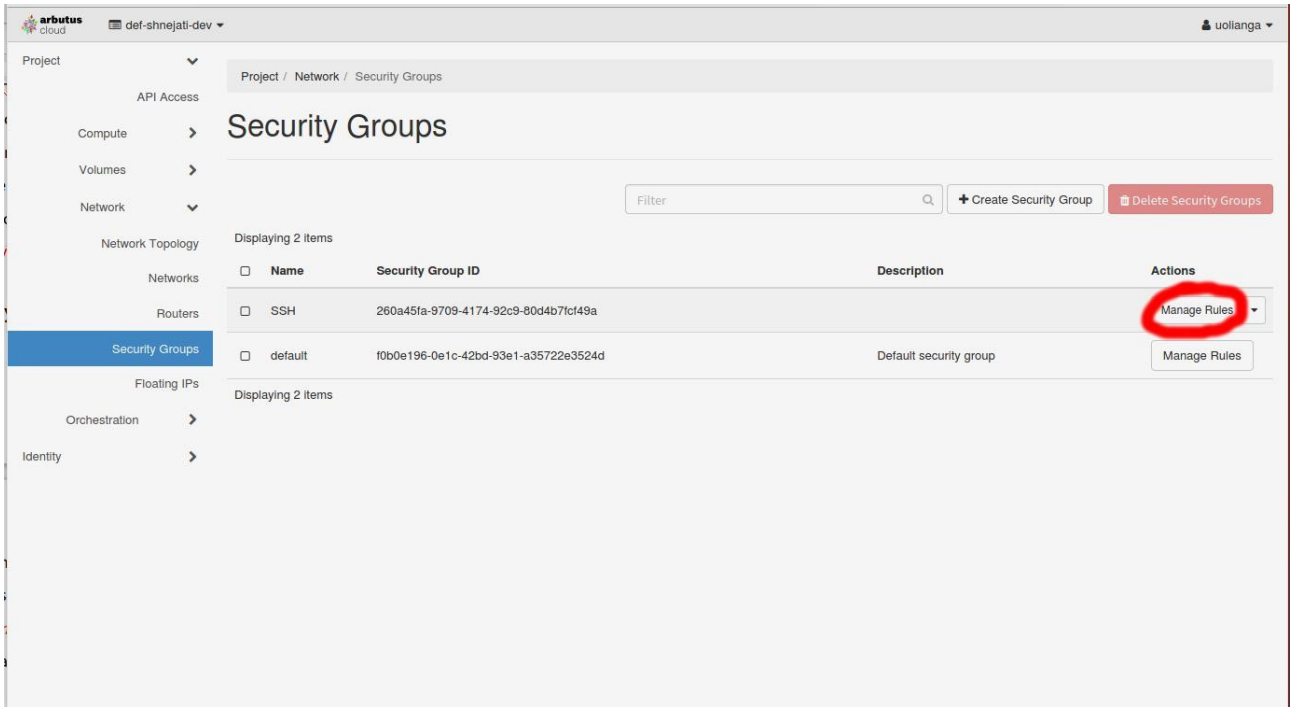
What type of the machines do we need to create?

In this project, we need only 2 nodes.

One is Manage machine (running ONOS) and the other one is Mininet machine (running Mininet). So, we need to create 2 machines on CCC.
The Manage machine is used to install 2 versions of DICES (Jenetics-DICES and ECJ-DICES) in ONOS and automatically deploy related environments on the Mininet machine.
For both Mininet machine and Manage machine, we use the image: *Ubuntu-18.04.3-Bionic-x64-2020-01*.

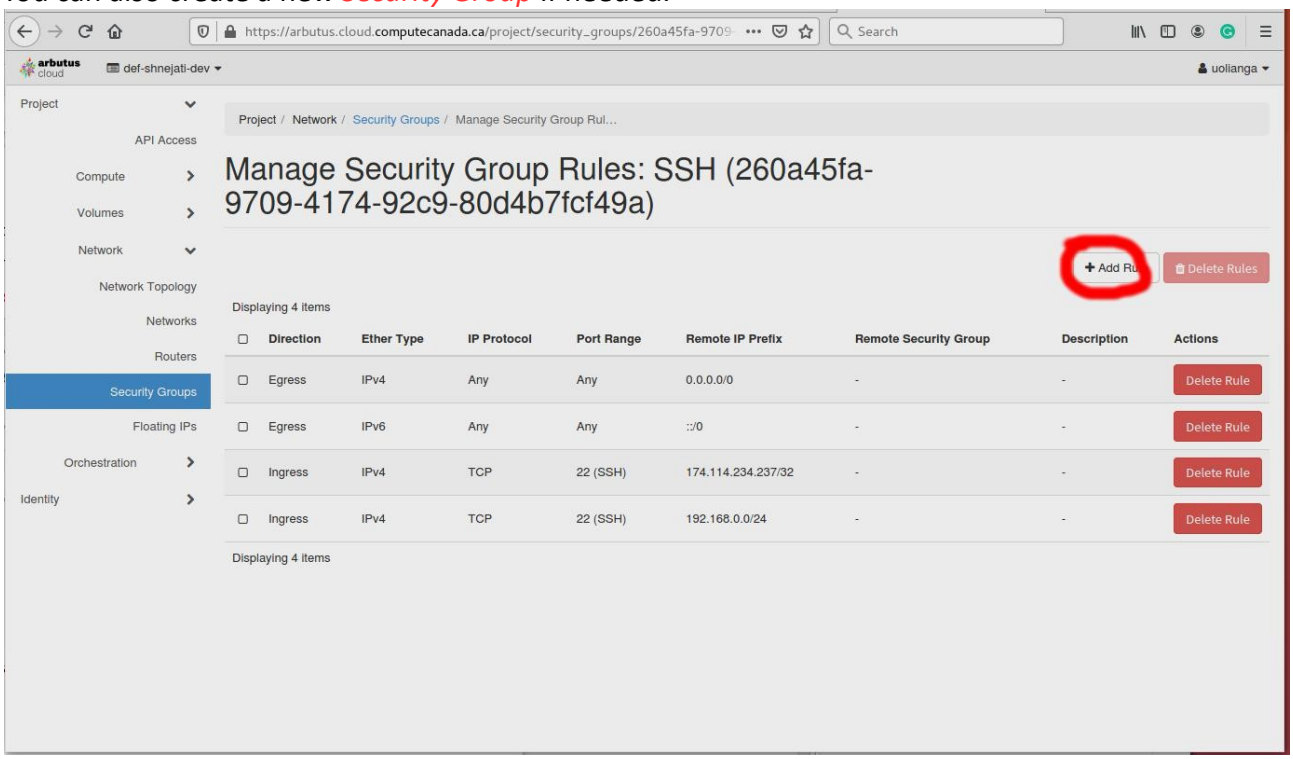
Deploy Security Group

We need to limit the specific IP address range that can connect to our machine in the security group and make sure that all the machines can communication with each other on the IP layer and can ssh to other machines.
Let us go to *Security Group* tab.

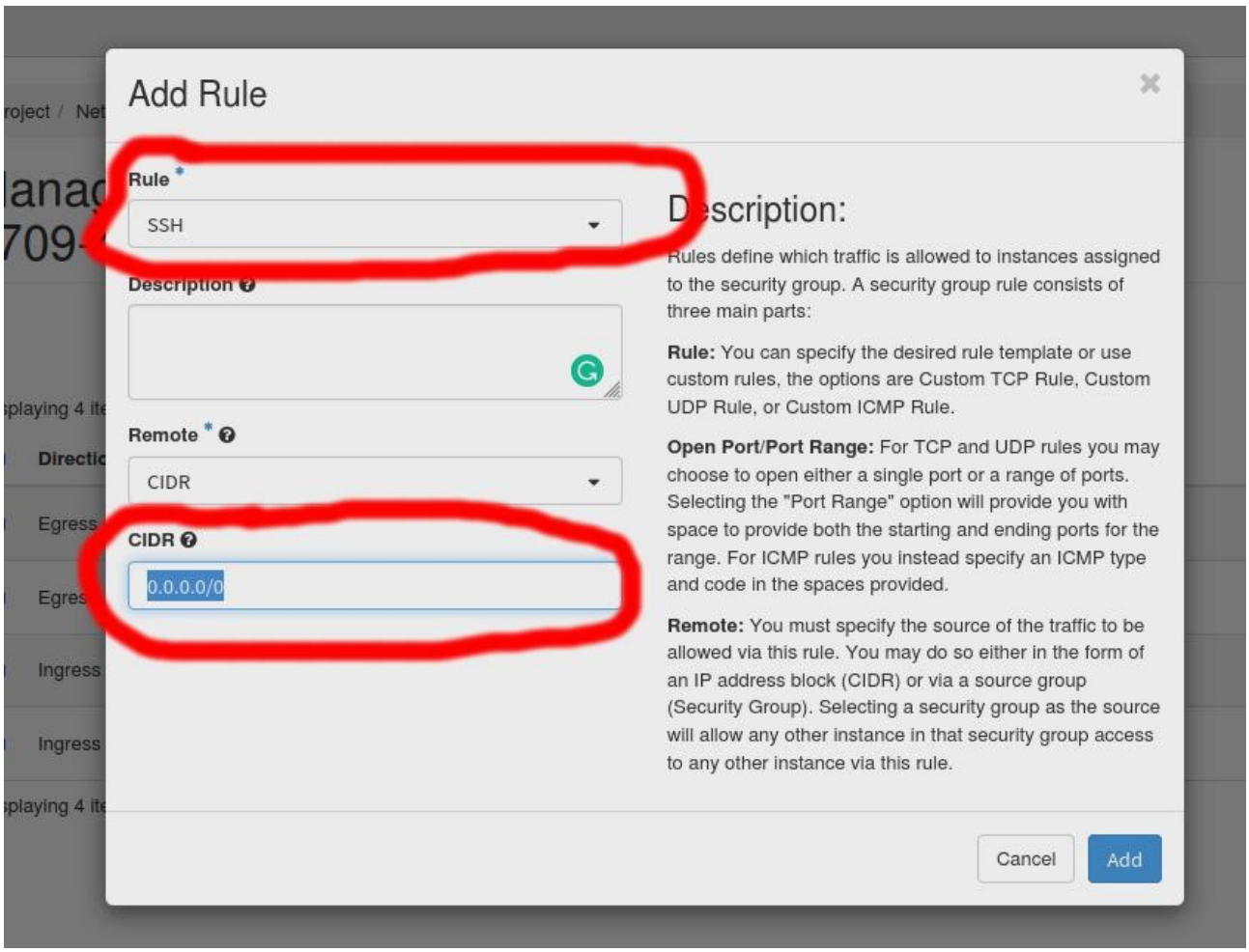


Because I already have a security group, you can use this, click *Manage Rule* button for Name *SSH*.

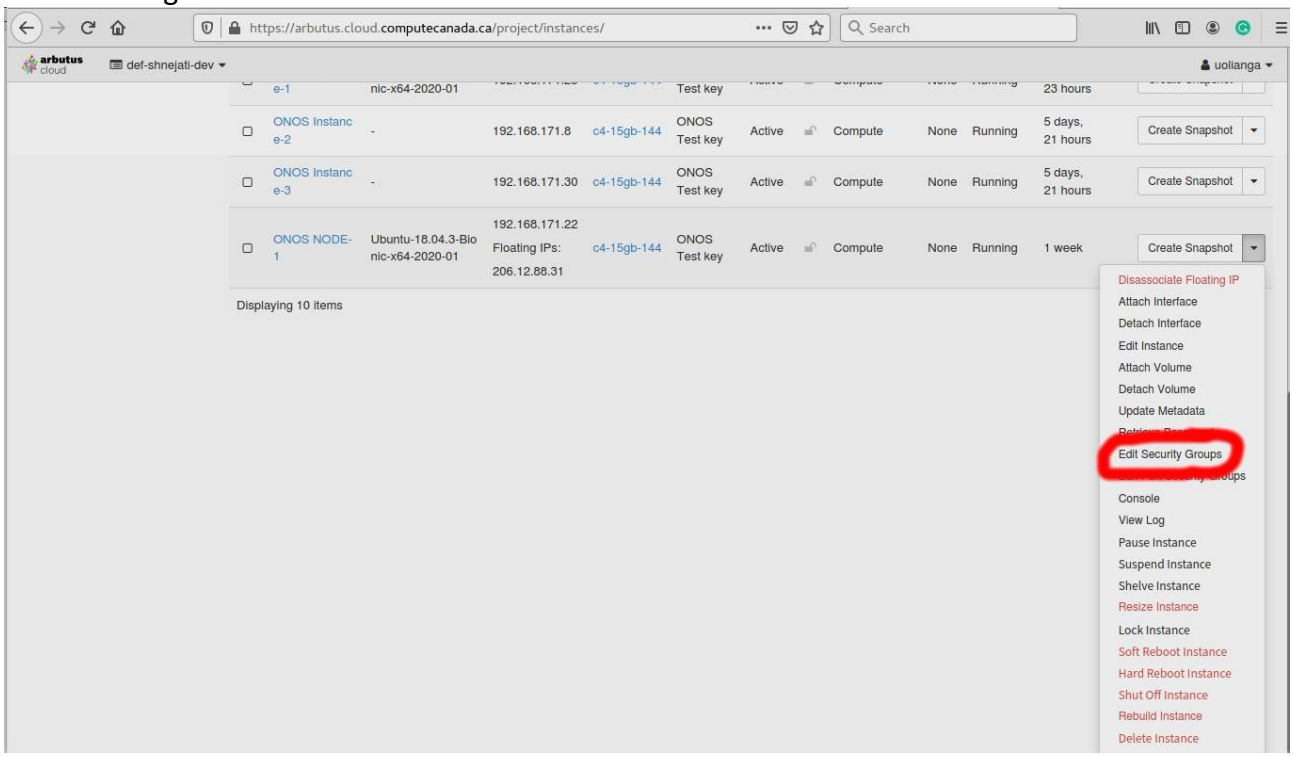
You can also create a new *Security Group* if needed.



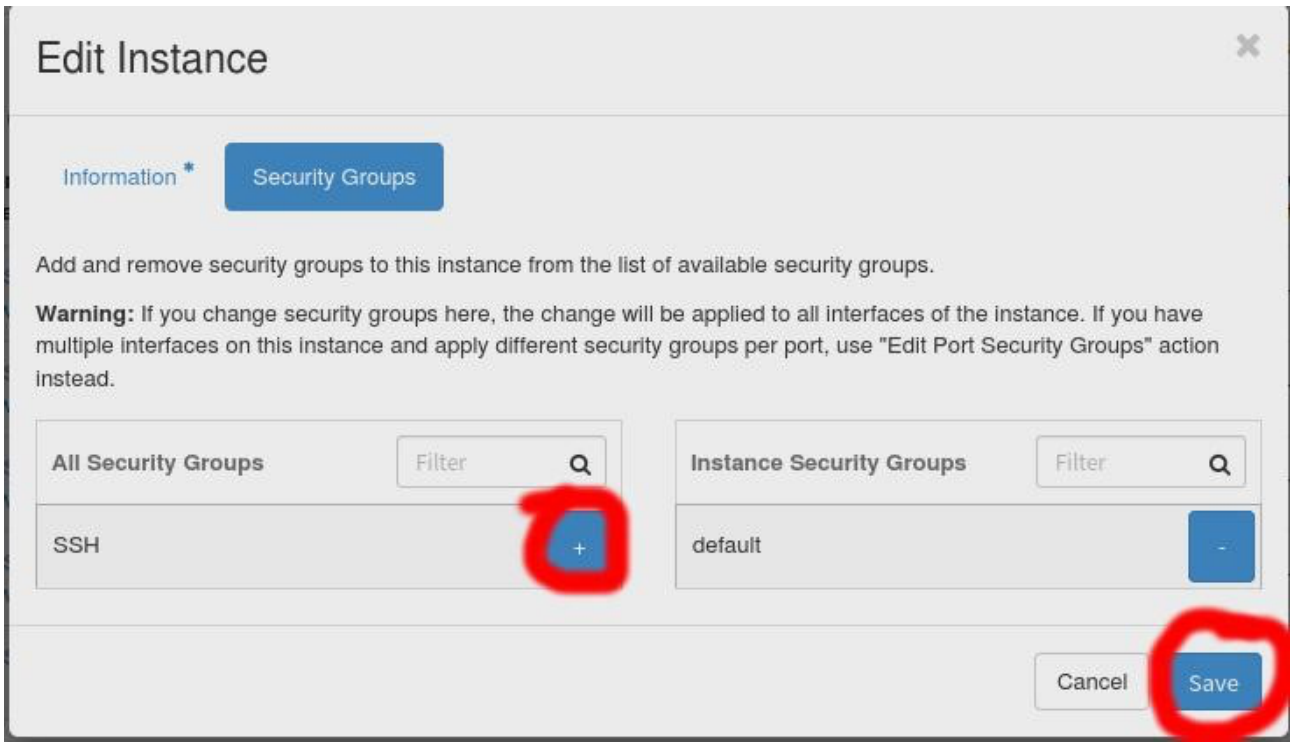
Click *Add rule* button.



Then change *Rule* to *SSH*. Change CIDR to *your IP address*. This will allow your address to connect to the Manage machine. Then we click *Add* to finish.

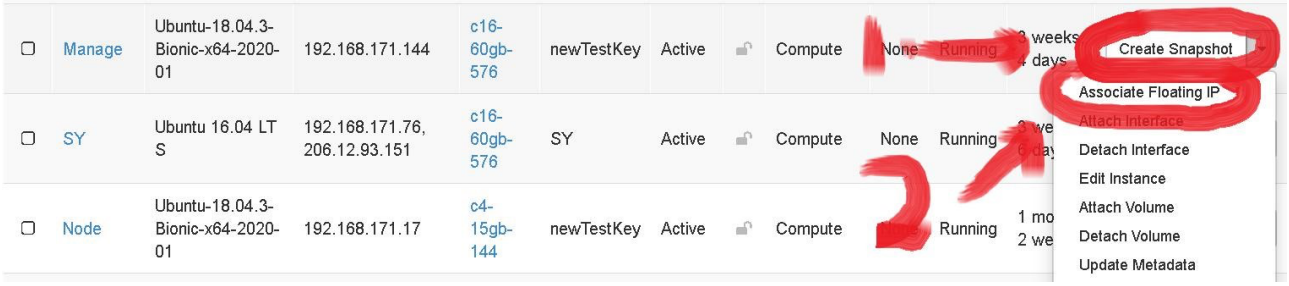


Go to *Instance* tab and click *Edit Security Group* (under Manage machine's drop-down menu) as shown.

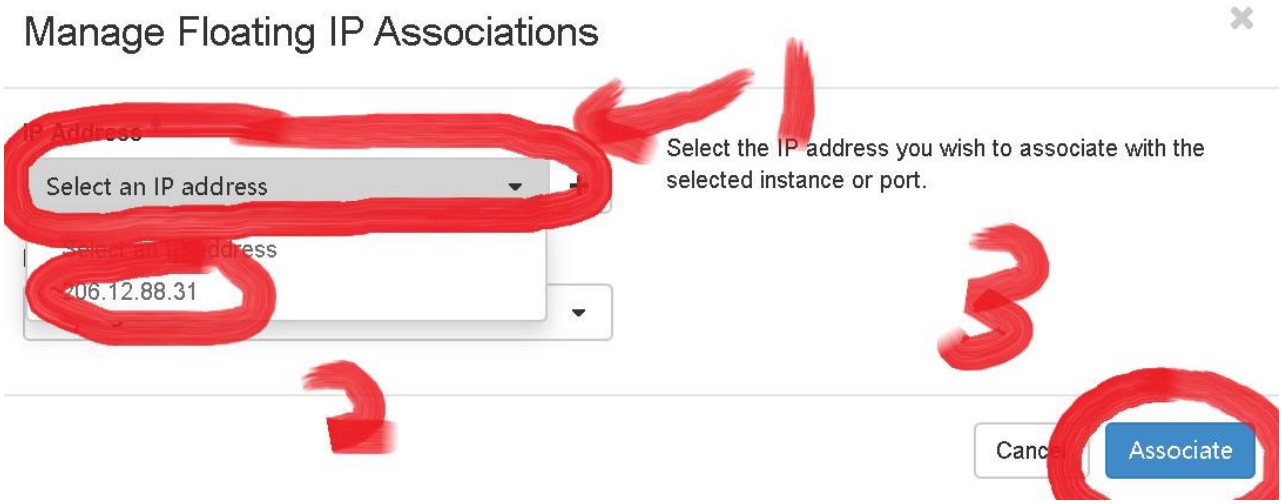


Click *"+"*button and *Save*.

Then, we need to give our *Instance* an A public IP address to connect (Note that only for **the Manage Machine**)

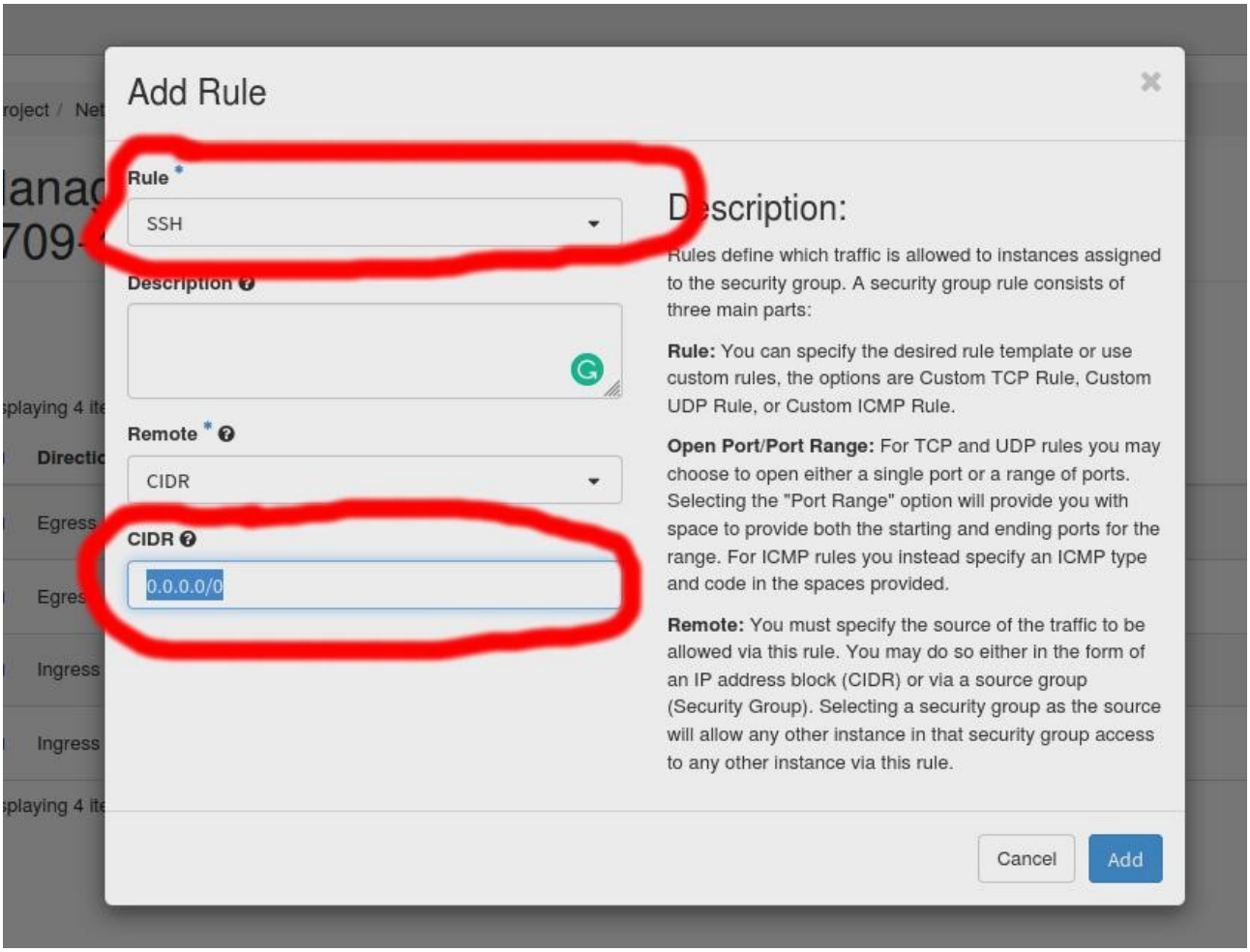


In the **Instances page**, click "Create Snapshot" then click "Associate Floating IP".



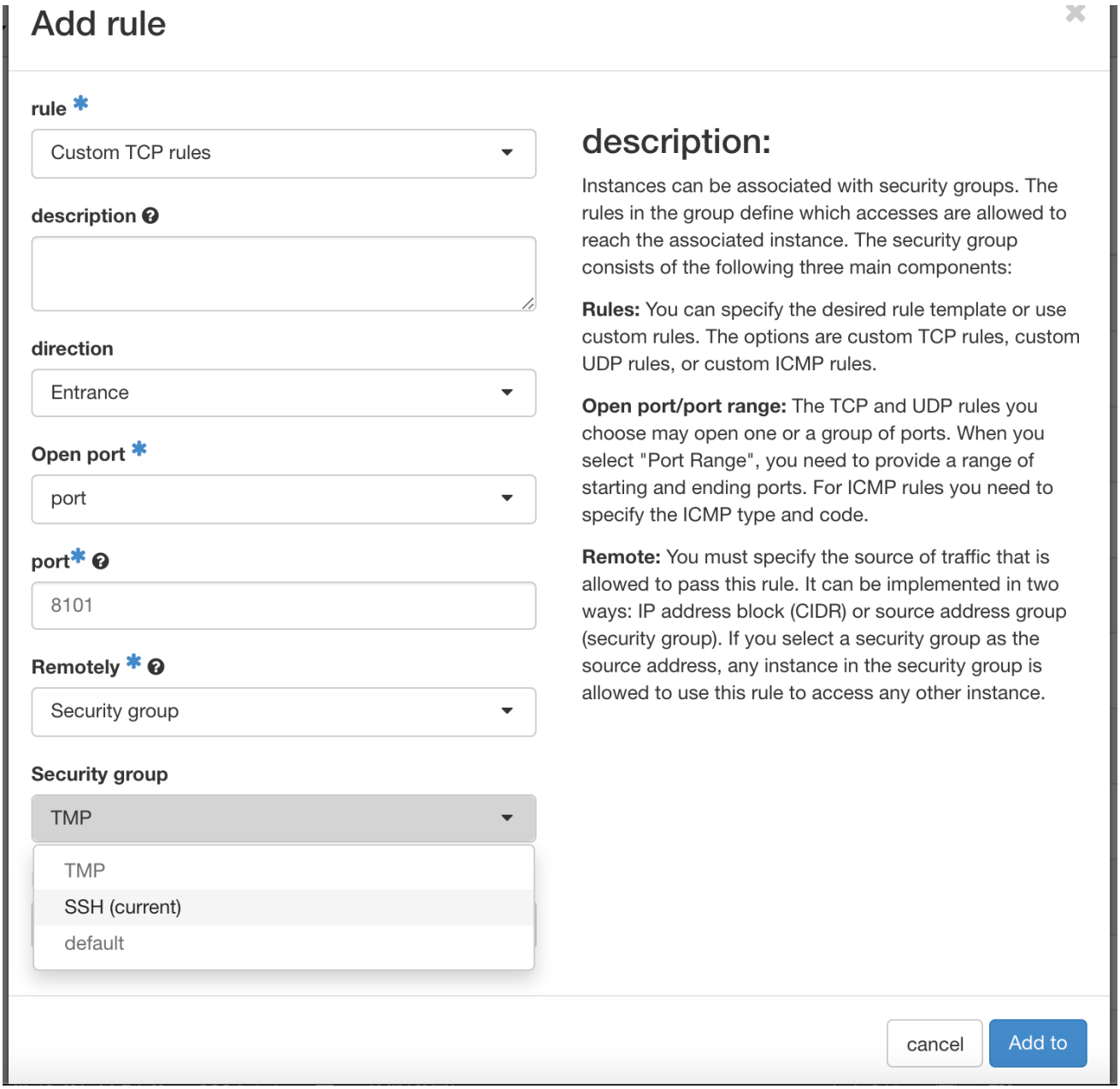
Click "Select an IP address", choose one ip address and then click "Associate".

Next, we should add SSH rules for **Mininet machine** and **Target machines**.



Go into the **same** security group and add rule. Change the *Rule* to *SSH* and change *CIDR* to your *Mininet machine's IP address* (intranet IP). Same for the Target machines. This step will make sure you can ssh from your Manage machine to all the machines.

Note: We also need to add some security group rules to open some **ports** for communication between manage Machine, Mininet machine and Target machines. We can go into the same security group and click *Add Rule* button.



Here we use port 8101 (for ONOS CLI session communication) as an example. The *Rule Type* is *Custom TCP rules*. We should create this rule for **both** directions (*Egress* and *Ingress*, which means we need to create 2 rules for 1 port). Then input the *port number* (8101). For the *Remote* option, we need to select the *Security group* option because it will make this port open for all the IP addresses that are included in this security group. After all the needed ports are added as rules, we Go to *Instance* tab and click *Edit Security Group* for every machine (Manage, Mininet and Target).

To find out which port should be opened, please refer to this page:
https://wiki.onosproject.org/display/ONOS/Requirements

Now everything is done and we can connect to our Manage machine by:

> *ssh -i <private key> ubuntu@<the Manage machine's ip address>*
>
> Or if your *<private key>* is located in ~/.ssh/, you can connect to it directly by:
> *ssh ubuntu@<the Manage machine's ip address>*

Then we can let the automation scripts do the job!