

# 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.

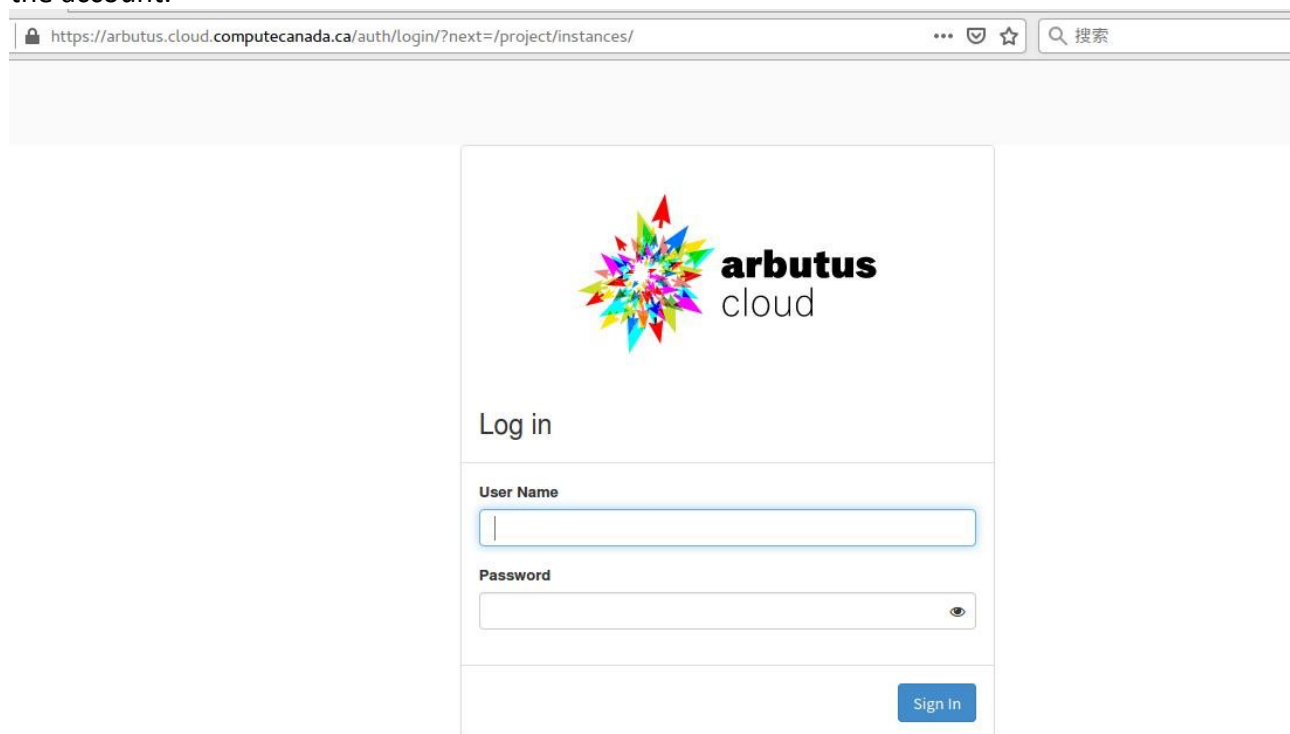
The Compute Canada Cloud service can provide researchers who require greater configurability, availability, durability clusters. Meanwhile, the cloud can provide researchers with virtual machines to meet their personal needs, including setting the size of RAM, setting the size of hard disk, setting the 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.



Project / Compute / Instances

## Instances

Instance ID =  Filter **Launch Instance** Delete Instances More Actions

Displaying 10 items

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
ONOS instanc e-new-4	Ubuntu-18.04.3-Bi onic-x64-2020-01	192.168.171.35	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	18 hours, 15 minutes	Create Snapshot
ONOS instanc e-new-1	Ubuntu-18.04.3-Bi onic-x64-2020-01	192.168.171.40	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	18 hours, 15 minutes	Create Snapshot
ONOS instanc e-new-2	Ubuntu-18.04.3-Bi onic-x64-2020-01	192.168.171.6	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	18 hours, 15 minutes	Create Snapshot
ONOS instanc e-new-3	Ubuntu-18.04.3-Bi onic-x64-2020-01	192.168.171.24	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	18 hours, 15 minutes	Create Snapshot
ONOS instanc e-4	Ubuntu-18.04.3-Bi onic-x64-2020-01	192.168.171.11	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	2 days	Create Snapshot
Mininet Machi ne	Ubuntu-18.04.3-Bi onic-x64-2020-01	192.168.171.28	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	4 days, 19 hours	Create Snapshot
ONOS instanc e-1	Ubuntu-18.04.3-Bi onic-x64-2020-01	192.168.171.25	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	4 days, 20 hours	Create Snapshot
ONOS instanc e-2	-	192.168.171.8	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	5 days, 18 hours	Create Snapshot
ONOS instanc e-3	-	192.168.171.30	c4-15gb-144	ONOS Test key	Active	Compute	None	Running	5 days, 18 hours	Create Snapshot

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

### Launch Instance

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

**Details**

Source \*

Flavor \*

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

**Instance Name \***

Newinstance

**Description**

The new ONOS node (target machine)

**Availability Zone**

Any Availability Zone

**Count \***

1

Total Instances (20 Max)

55%

10 Current Usage

1 Added

9 Remaining

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.

Details

Source \*

Flavor \*

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source

Image

Create New Volume

Yes

No

Allocated

Name	Updated	Size	Type	Visibility
Select an item from Available items below				

▼ Available 8

Select one

Q Click here for filters.

Name	Updated	Size	Type	Visibility	
> CentOS-7-x64-2019-07	1/17/20 3:54 PM	898.75 MB	qcow2	Public	⬆
> CentOS-8-x64-2019-11	1/17/20 3:53 PM	683.00 MB	qcow2	Public	⬆
> Debian-10.2.0-Buster-2019-11	1/17/20 3:54 PM	540.19 MB	qcow2	Public	⬆
> Fedora-30-1.2-x86-2019-07	1/17/20 3:56 PM	316.88 MB	qcow2	Public	⬆
> Fedora-31-1.9-x64-2020-01	1/17/20 3:54 PM	338.89 MB	qcow2	Public	⬆
> Ubuntu-18.04.3-Bionic-minimal-x64-2020-01	1/17/20 3:54 PM	160.94 MB	qcow2	Public	⬆
> Ubuntu-18.04.3-Bionic-x64-2020-01	1/17/20 3:54 PM	329.06 MB	qcow2	Public	⬆
> Ubuntu-20.04-focal-amd64	6/3/20 4:30 PM	489.44 MB	qcow2	Public	⬆

✕ Cancel

< Back

Next >

Launch Instance

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.

Launch Instance

Details \*  
Source \*  
**Flavor \***  
Networks  
Network Ports  
Security Groups  
Key Pair  
Configuration  
Server Groups  
Scheduler Hints  
Metadata

Flavors manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
Select an item from Available items below						

▼ Available 13

Click here for filters.

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
> c1-7.5gb-36	1	7.5 GB	56 GB	20 GB	36 GB	No
> c2-7.5gb-36	2	7.5 GB	56 GB	20 GB	36 GB	No
> c2-15gb-72	2	15 GB	92 GB	20 GB	72 GB	No
> c4-15gb-144	4	15 GB	164 GB	20 GB	144 GB	No
> c8-30gb-288	8	30 GB	308 GB	20 GB	288 GB	No
> c4-30gb-144	4	30 GB	164 GB	20 GB	144 GB	No
> c4-45gb-144	4	45 GB	164 GB	20 GB	144 GB	No
> c8-60gb-288	8	60 GB	308 GB	20 GB	288 GB	No

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.

Launch Instance

Details \*  
Source \*  
Flavor \*  
Networks  
Network Ports  
Security Groups  
**Key Pair**  
Configuration  
Server Groups  
Scheduler Hints  
Metadata

A key pair allows you to SSH into your newly created instance. You may select an existing key pair, import a key pair, or generate a new key pair.

+ Create Key Pair Import Key Pair

Allocated

Displaying 0 items

Name	Fingerprint
Select a key pair from the available key pairs below.	

Displaying 0 items

▼ Available 2

Click here for filters.

Displaying 2 items

Name	Fingerprint
> liangli07	4f:03:fc:89:26:3e:1b:2a:64:63:8a:eb:7c:be:95:78
> ONOS Test key	ee:fb:c5:e0:d7:d9:c5:62:54:4c:bf:b1:65:c1:ac:8c

Displaying 2 items

Cancel < Back Next > Launch Instance

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.

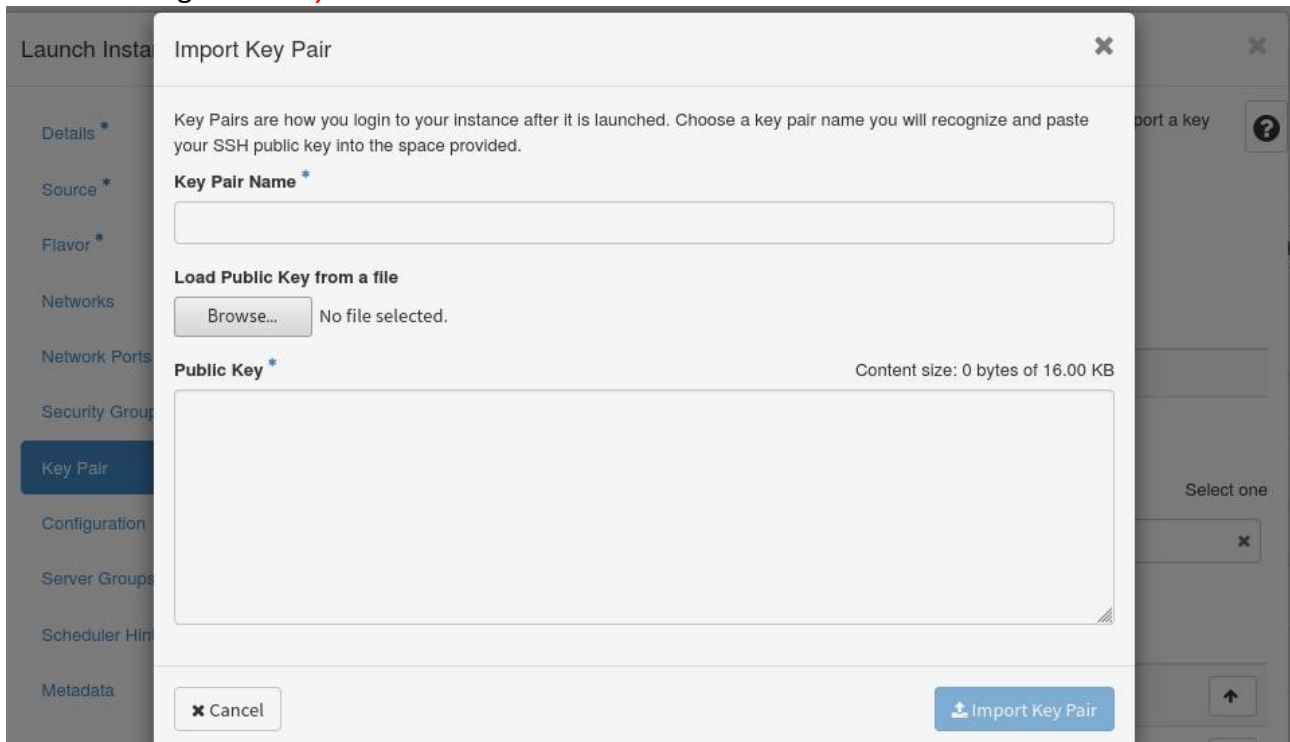
Optional:

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.

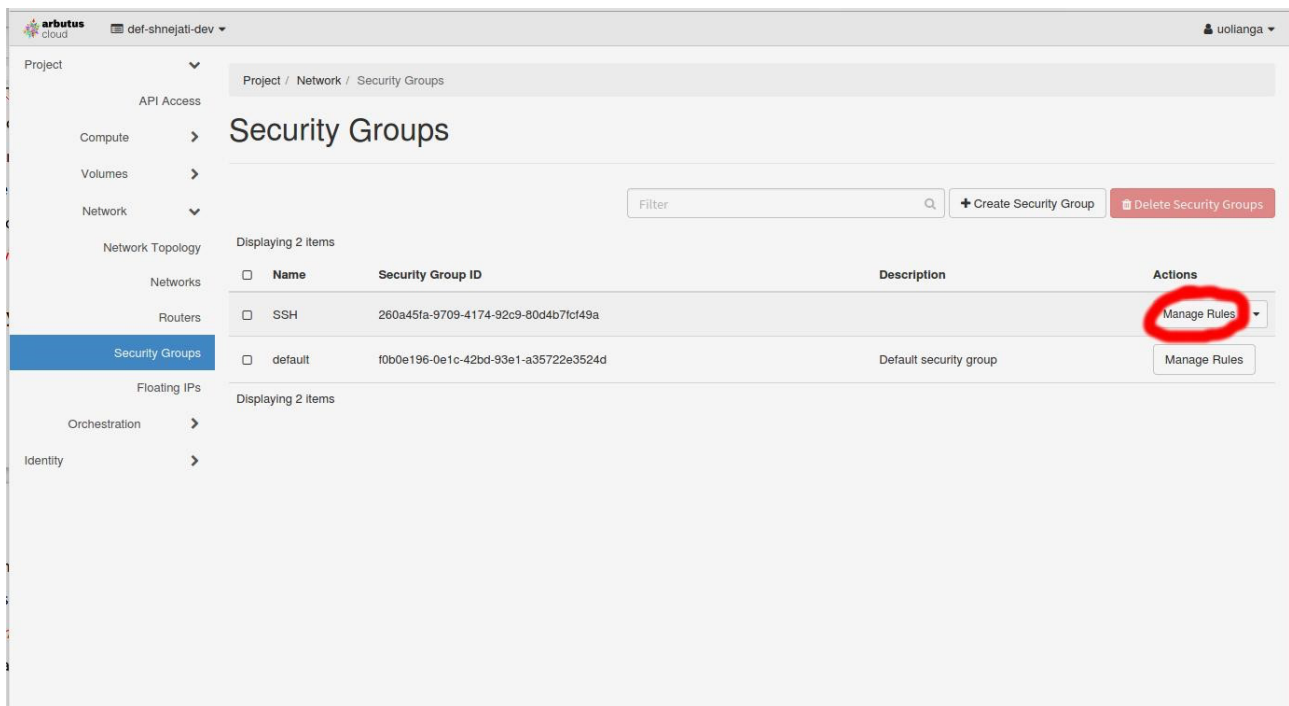
For both Mininet machine and Manage machine, we use the image: *Ubuntu-*

*18.04.3-Bionic-x64-2020-01*.

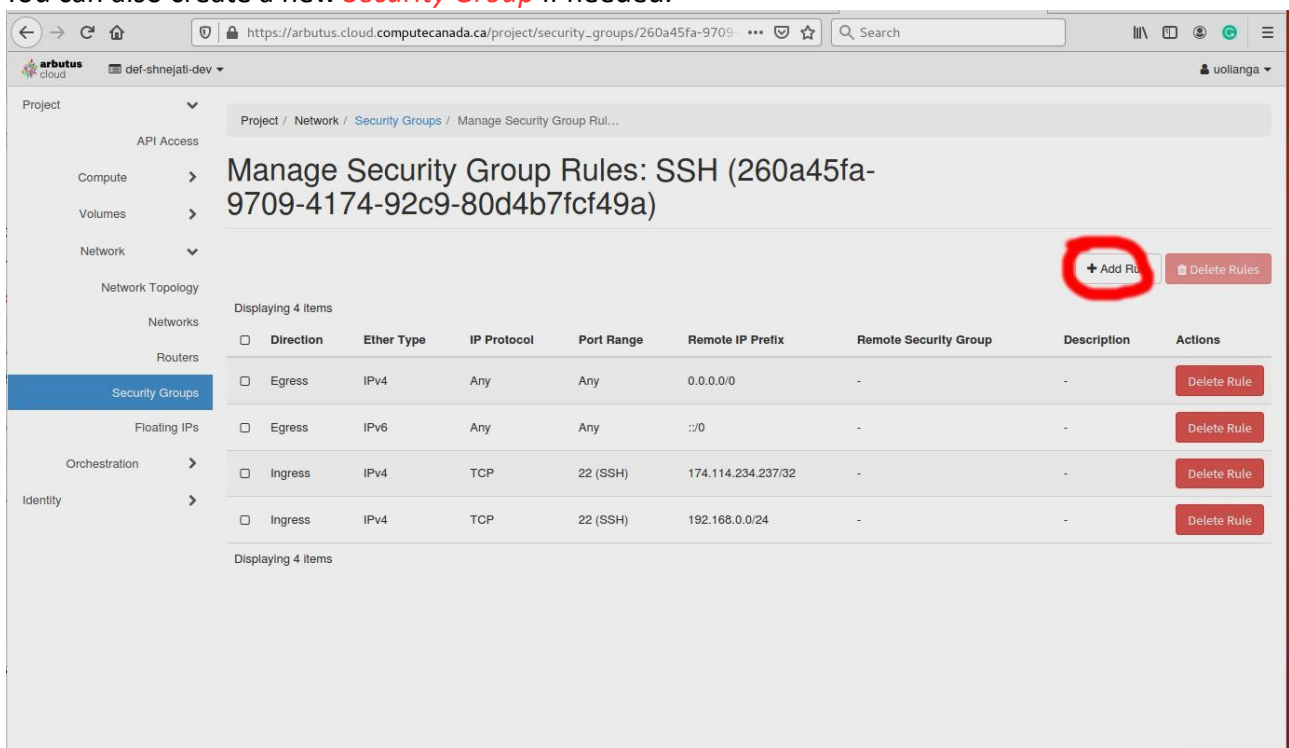
## Deploy Security Group

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.



**Add Rule**

**Rule**  
SSH

**Description**

**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.

Cancel Add

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.

arbutus cloud

def-shnejati-dev

Instance	OS	IP	Key	Status	Group	Plan	Time	Actions
ONOS Instance e-1	Ubuntu-18.04.3-Bionic	192.168.171.8	Test key	Active	Compute	None	Running	5 days, 21 hours
ONOS Instance e-2	Ubuntu-18.04.3-Bionic	192.168.171.30	Test key	Active	Compute	None	Running	5 days, 21 hours
ONOS Instance e-3	Ubuntu-18.04.3-Bionic	192.168.171.30	Test key	Active	Compute	None	Running	5 days, 21 hours
ONOS NODE-1	Ubuntu-18.04.3-Bionic	192.168.171.22	Test key	Active	Compute	None	Running	1 week

Displaying 10 items

Disassociate Floating IP  
Attach Interface  
Detach Interface  
Edit Instance  
Attach Volume  
Detach Volume  
Update Metadata  
Edit Security Groups

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

## Edit Instance

Information \* Security Groups

Add and remove security groups to this instance from the list of available security groups.

**Warning:** If you change security groups here, the change will be applied to all interfaces of the instance. If you have multiple interfaces on this instance and apply different security groups per port, use "Edit Port Security Groups" action instead.

All Security Groups
Filter
SSH
+

Instance Security Groups
Filter
default
-

Cancel Save

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**)

<input type="checkbox"/>	Manage	Ubuntu-18.04.3-Bionic-x64-2020-01	192.168.171.144	c16-60gb-576	newTestKey	Active	Compute	None	Running	3 weeks 4 days	Create Snapshot
<input type="checkbox"/>	SY	Ubuntu 16.04 LTS	192.168.171.76, 206.12.93.151	c16-60gb-576	SY	Active	Compute	None	Running	2 weeks 6 days	Associate Floating IP
<input type="checkbox"/>	Node	Ubuntu-18.04.3-Bionic-x64-2020-01	192.168.171.17	c4-15gb-144	newTestKey	Active	Compute	None	Running	1 month 2 weeks	Attach Interface

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

## Manage Floating IP Associations

IP Address \*

Select an IP address

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

206.12.88.31

Cancel Associate

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**.



**Add Rule**

**Rule**  
SSH

**Description**

**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.

Cancel Add

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.

