OpenStack Installation Guide - PackStack

1 Prepare the physical machines

1.1 Hardware

One network adapter that can access external network, i.e., ping google.com successfully.

1.2 Install OS

The OS is CentOS 6.5.

Several notes

1. Choose **minimal** installation
2. Assign a hostname such as server1.comapny
3. Do NOT configure network

1.3 Post-installation

After reboot, configure the network interface using static IP

```
# ifcfg-em1
DEVICE=em1
HWADDR=D4:AE:52:CA:F3:46
TYPE=Ethernet
UUID=36ca35ae-ddf9-4789-9a15-89fe1b6fa977
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=static
IPADDR=10.1.10.112
NETMASK=255.255.255.0
GATEWAY=10.1.10.1
```

```
# Disable firewall, selinux, NetworkManager, and iptables
# Enable network
# reboot
```

This state is called bare-metal. Reboot the machine.

1.4 Check static network

After rebooting, make sure the network functions correctly. Edit /etc/hosts. Add hostname and IP to the file.

```
# ping google.com to make sure the network is correct.

# hostname -f
```

2 Install RDO openstack Havana

```
# yum install -y http://rdo.fedorapeople.org/rdo-release.rpm
```

```
# yum install -y openstack-packstack
```

```
# yum update
# reboot
```

2.1 Check network and hostname

Before proceeding to the next step, make sure that the machine can access external network and hostname is set correctly.

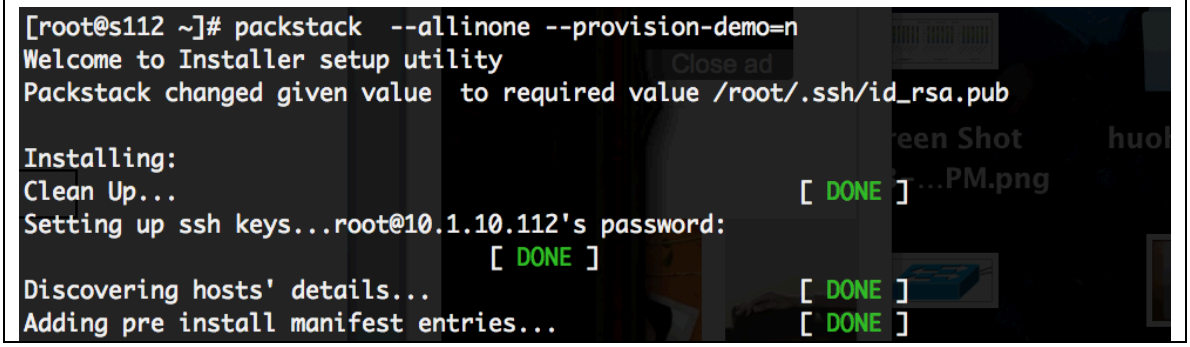
```
# ping google.com

# hostname -f  return correct hostname
```

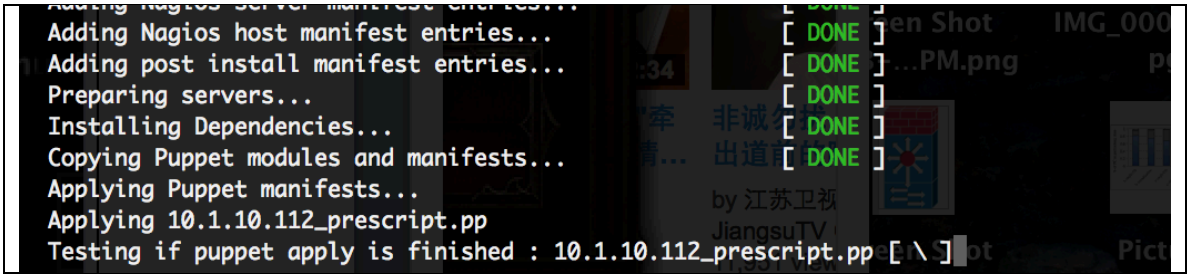
2.2 Install openstack by packstack

Now you can install openstack on the machine

```
# packstack  --allinone --provision-demo=n
```



It will take some time. So get a cup of coffee and wait.



If everything goes well, you will see this

```
10.1.10.112_postscript.pp :                    [ DONE ]
                                   [ DONE ]
Finalizing...                                          [ DONE ]

**** Installation completed successfully ******
                                                  did you see my we chat message

Additional information:
 * A new answerfile was created in: /root/packstack-answers-20140222-174026.txt
 * Time synchronization installation was skipped. Please note that unsynchronized tim
e on server instances might be problem for some OpenStack components.
 * File /root/keystonerc_admin has been created on OpenStack client host 10.1.10.112.
To use the command line tools you need to source the file.
 * To access the OpenStack Dashboard browse to http://10.1.10.112/dashboard.
Please, find your login credentials stored in the keystonerc_admin in your home direc
tory.
 * To use Nagios, browse to http://10.1.10.112/nagios username : nagiosadmin, passwor
```

3 Configure Network

```
# ifcfg-br-ex, created by packstack
DEVICE=br-ex
DEVICETYPE=ovs
TYPE=OVSBridge
BOOTPROTO=static
IPADDR=10.1.10.107
NETMASK=255.255.255.0
ONBOOT=yes
GATEWAY=10.1.10.1
```

```
# ifcfg-em1, the physical NIC
DEVICE=em1
HWADDR=XX:XX  # mac address
TYPE=OVSPort
DEVICETYPE=ovs
OVS_BRIDGE=br-ex
ONBOOT=yes
```

3.1 Restart network

```
# service network restart
```

Test if the machine can still access external network. If not set the default gateway to br-ex.

```
# ping google.com

# hostname -f  return correct hostname
```

4 Dashboard configuration

Open a browser and point to

```
http://10.1.10.112/dashboard/
```

User name is “admin” and password is located at “/root/keystonerc_admin”.

4.1 Select the hypervisr on compute node (ignore this step if on a physical machine)

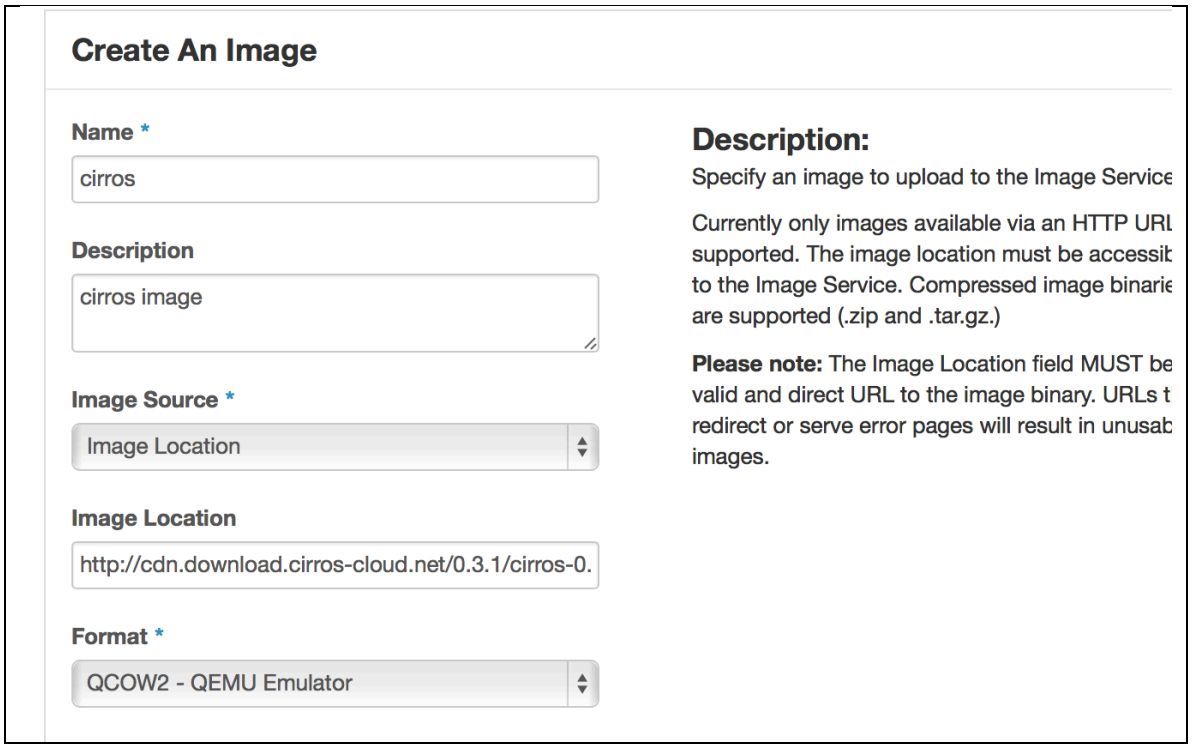
If you are testing compute node in a virtual machine (virtual box environment), you must not use qemu-kvm. So edit the /etc/nova/nova.cnf

```
compute_driver=libvirt.LibvirtDriver
libvirt_type=qemu
```

Re-boot the compute node

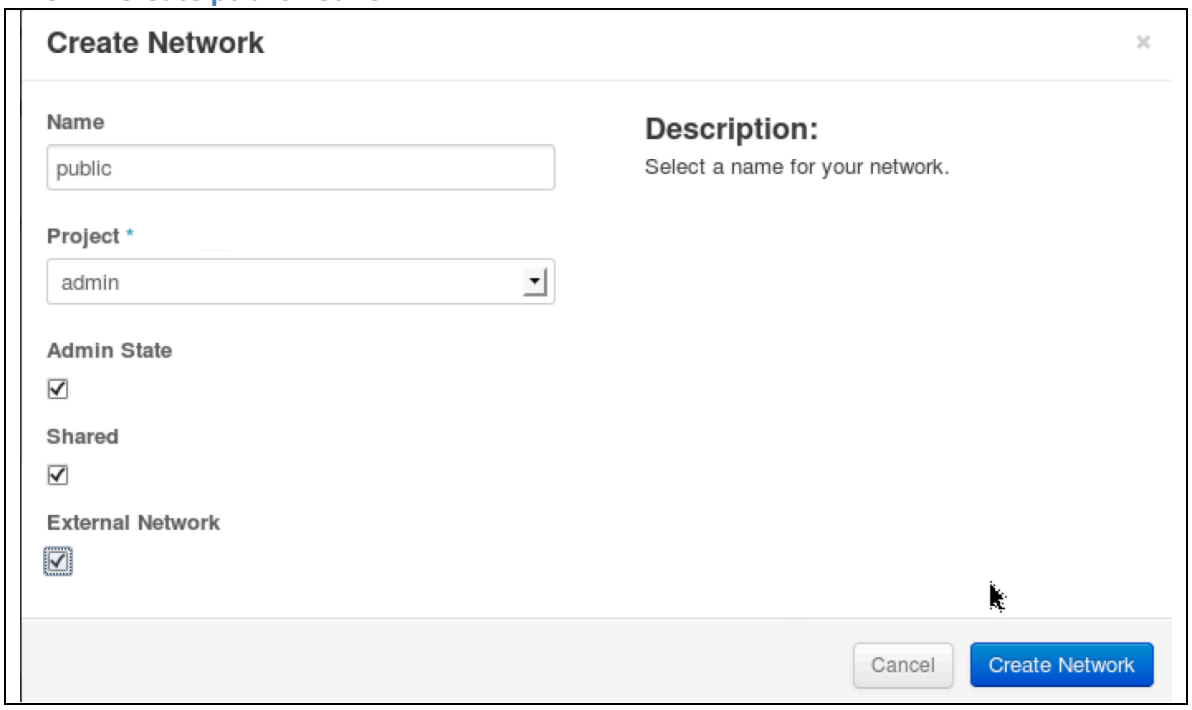
4.2 Update image

```
http://cdn.download.cirros-cloud.net/0.3.1/cirros-0.3.1-x86_64-disk.img
```

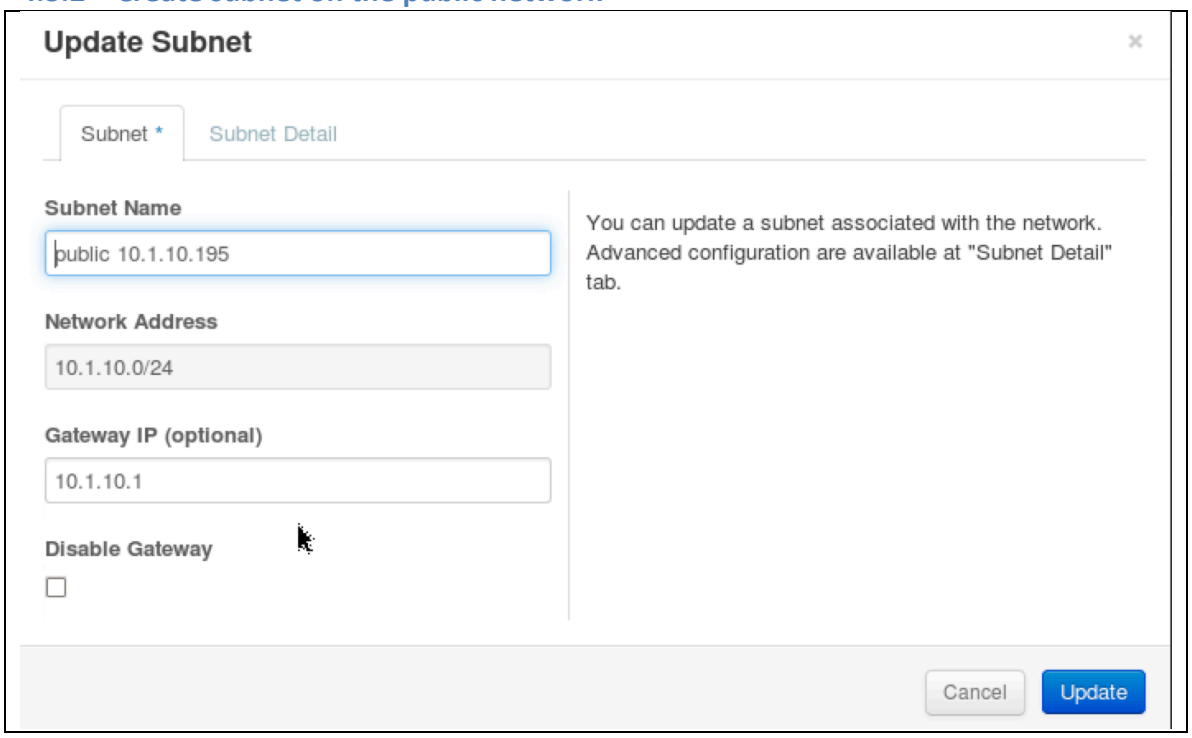


4.3 Create public, private networks, and router

4.3.1 Create public network

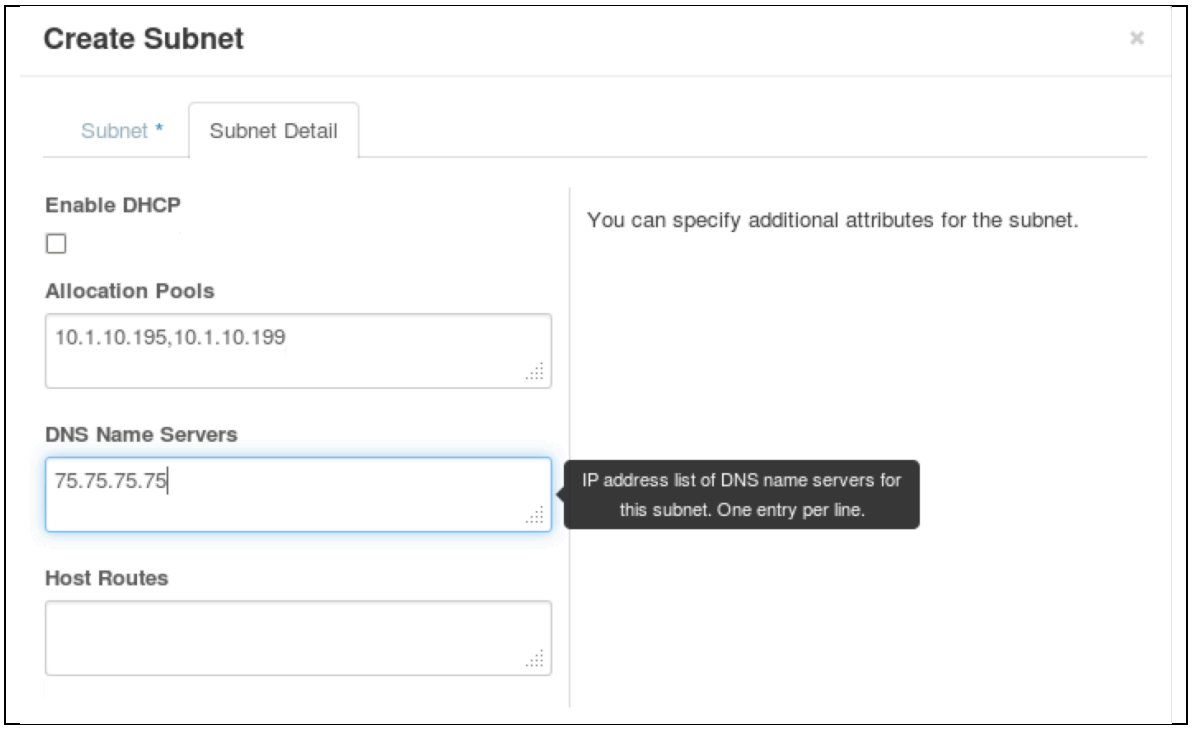


4.3.2 Create subnet on the public network



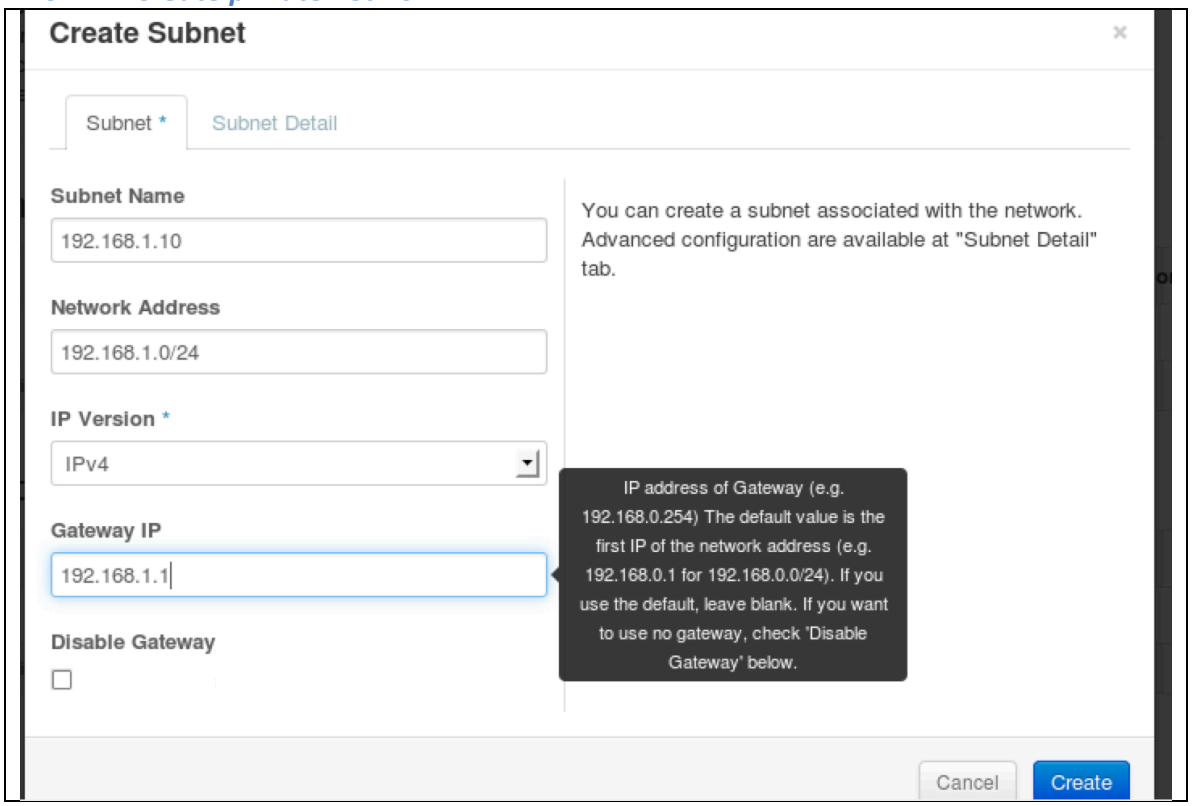
4.3.3 Subnet detail

We assign 195 to 199 as the floating IP addresses to the VMs. DHCP must not be enabled.



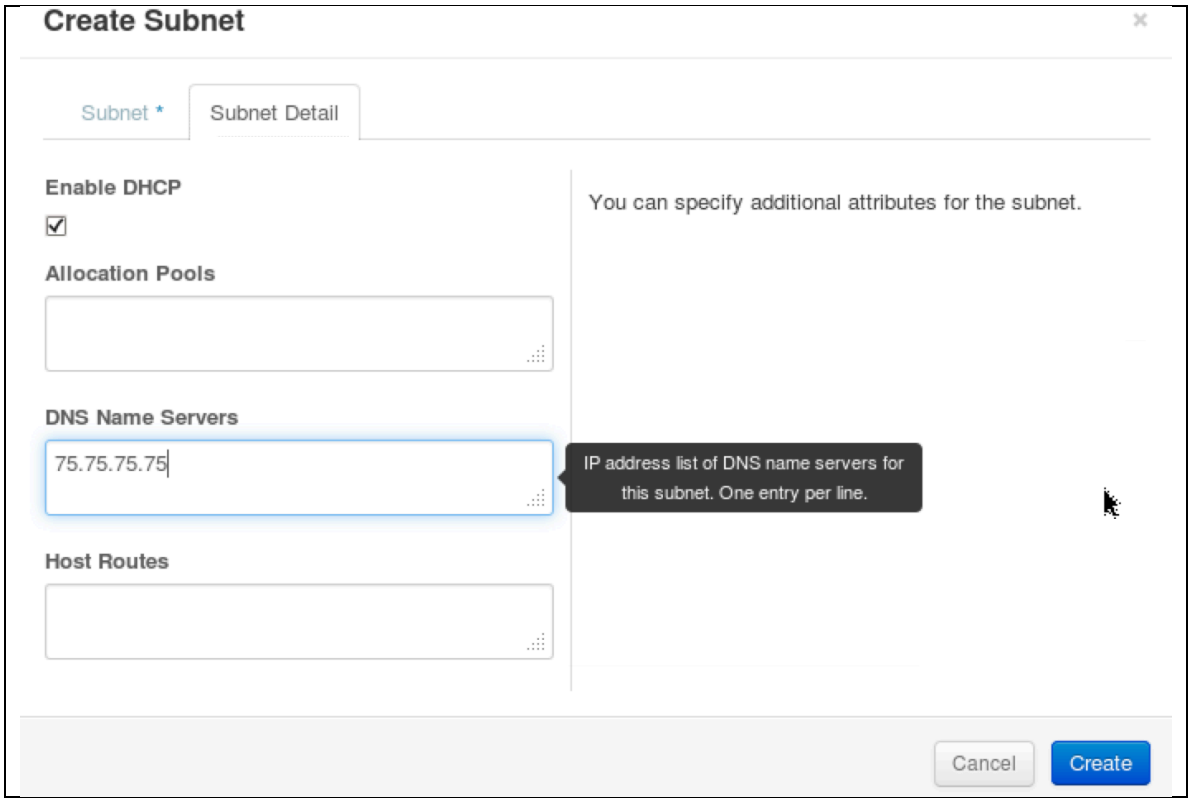
4.3.4 Private network

4.3.4.1 Create private network



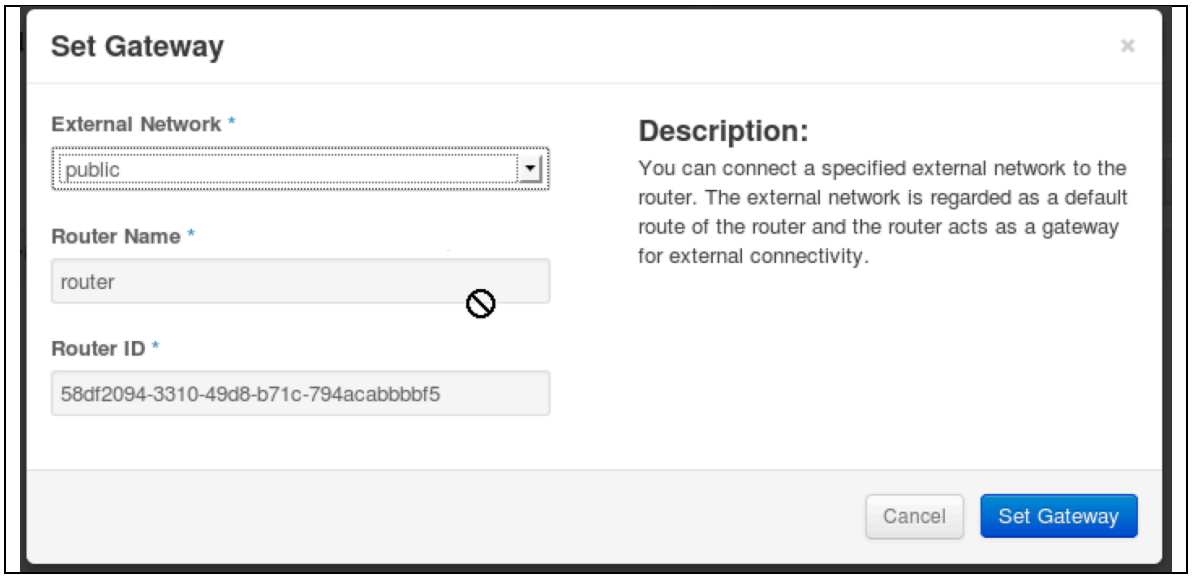
4.3.4.2 Subnet detail

For private, you need to enabled DHCP.

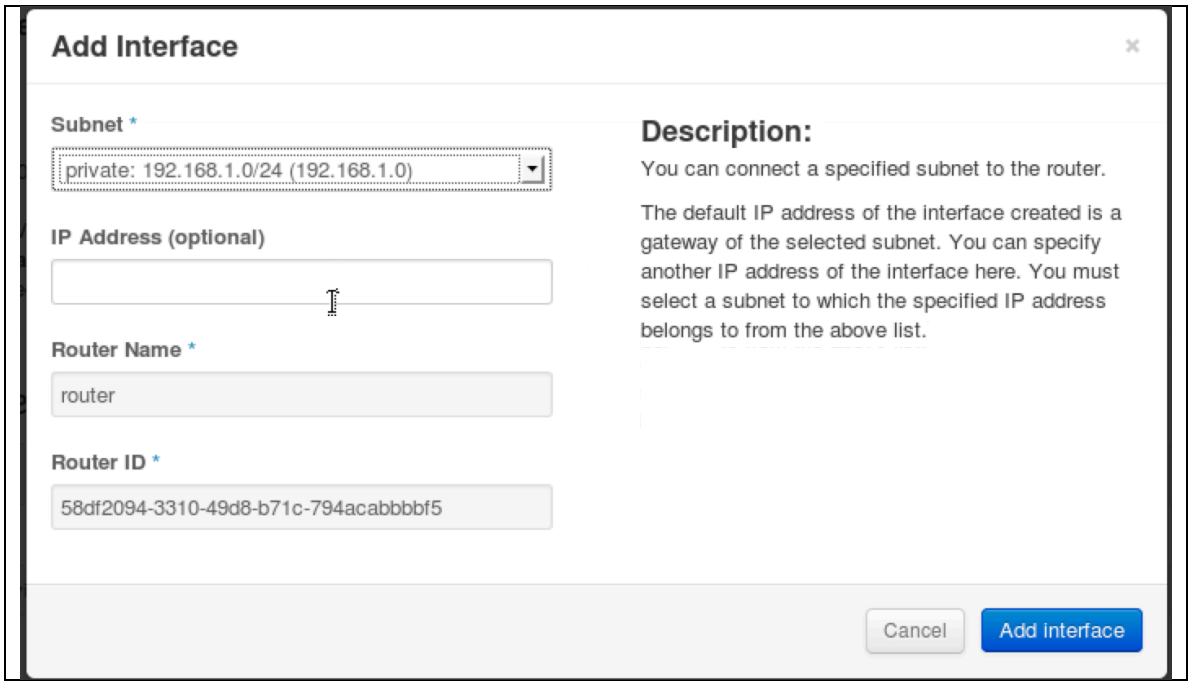


4.3.5 Create router

Set the router gateway to the public network



Attach the private network to the router, as its interface



4.4 Setup ICMP and ssh security rule

Edit default security rule

Add Rule

Rule *

Custom TCP Rule

Direction

Ingress

Open Port *

Port

Port

22

Enter an integer value between 1 and 65535.

Remote *

CIDR

CIDR

0.0.0.0/0

Description:

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

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

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

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

Add Rule

Rule *

Custom ICMP Rule

Direction

Ingress

Type

-1

Code

-1

Enter a value for ICMP code in the range (-1: 255)

Remote *

CIDR

CIDR

Description:

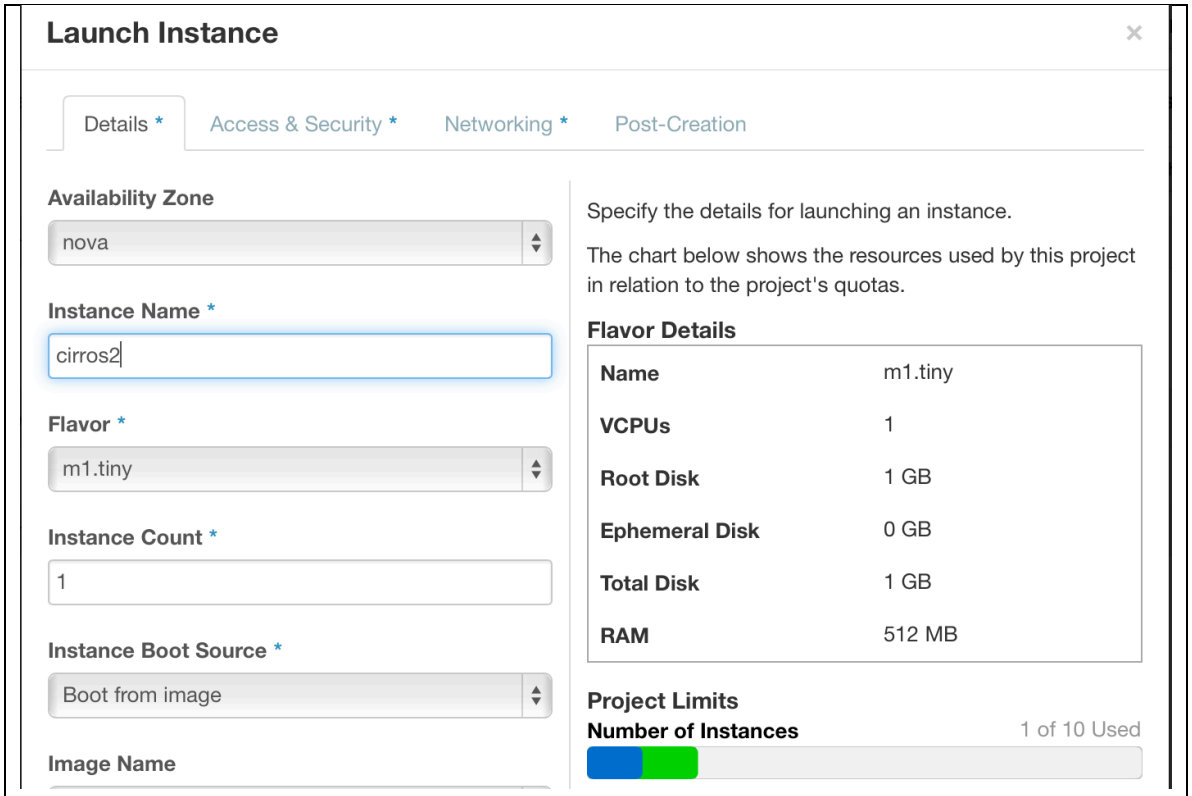
Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

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.

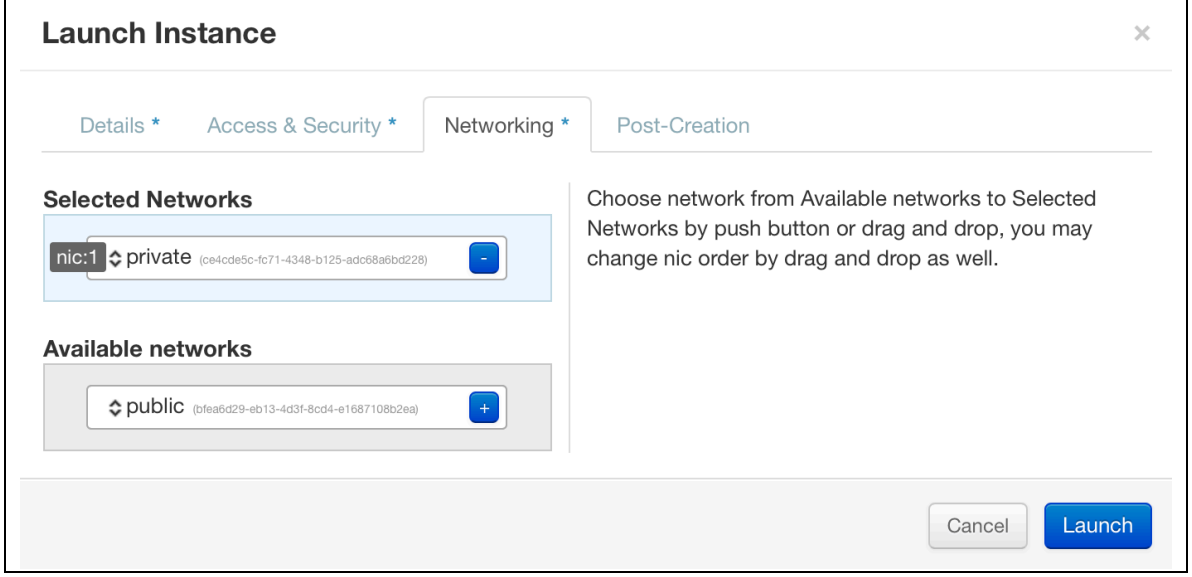
Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and For ICMP rules you instead ify an ICMP type and code in the spaces provided.

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

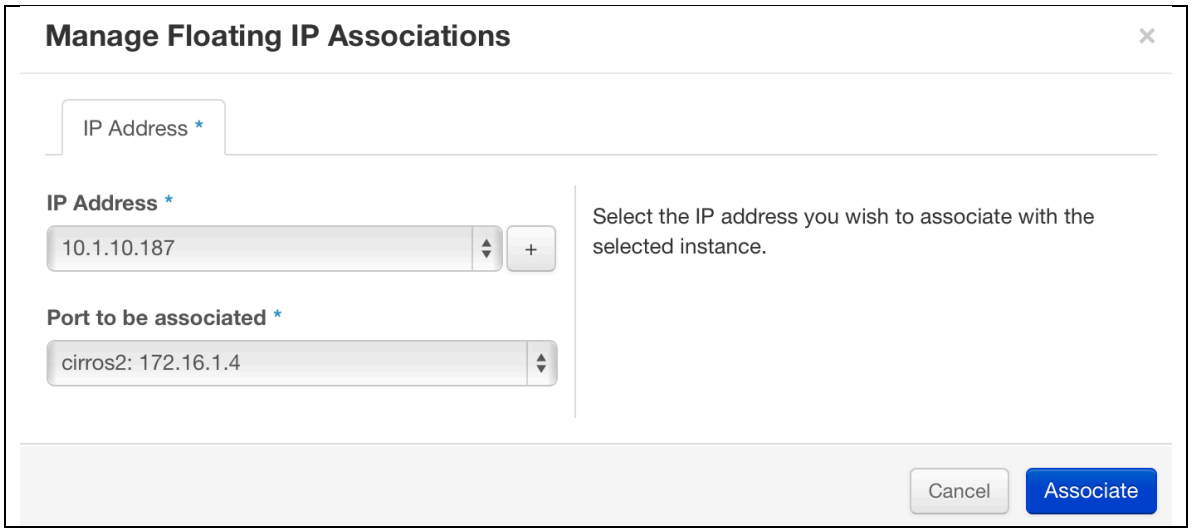
4.5 Launce instance



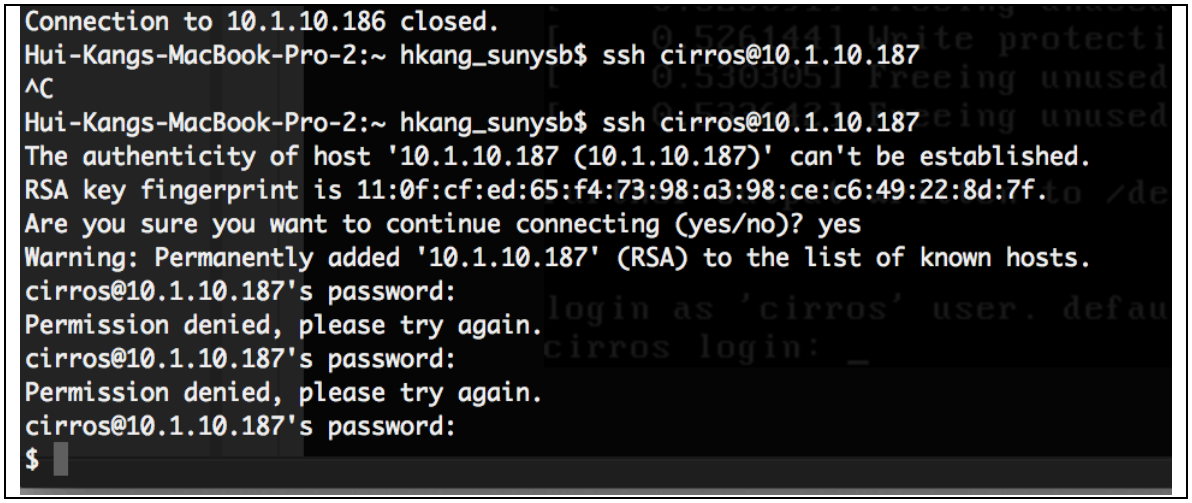
Setup network for the instance



Now associate a floating IP to the VM



Now we can ping this vm using the floating IP from any host in the public network. The username to the cirros is “cirros” and password is “cubswin:)”. To use root, type “sudo -i”.



5 Trouble shooting

(a) check if the compute node can ping google? Check the hostname of the compute node.

6 Reference

[1] Openstack all in one in Chinese, http://www.chenshake.com/centos6-4-single-card-all-in-one-install-havana/