

OpenStack Installation Guide - PackStack

1	Prepare the physical machines.....	1
1.1	Hardware.....	1
1.2	Install OS.....	1
1.3	Post-installation	2
1.4	Check static network.....	2
2	Install RDO openstack Havana.....	2
2.1	Check network and hostname	3
2.2	Install openstack by packstack	3
3	Configure Network	4
3.1	Restart network.....	4
4	Dashboard configuration	5
4.1	Select the hypervisor on compute node (ignore this step if on a physical machine)	5
4.2	Update image	5
4.3	Create public, private networks, and router	6
4.3.1	Create public network.....	6
4.3.2	Create subnet on the public network	7
4.3.3	Subnet detail.....	7
4.3.4	Private network	8
4.3.5	Create router	9
4.4	Setup ICMP and ssh security rule	10
4.5	Launch instance	12
5	Trouble shooting	13
6	Reference	13

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

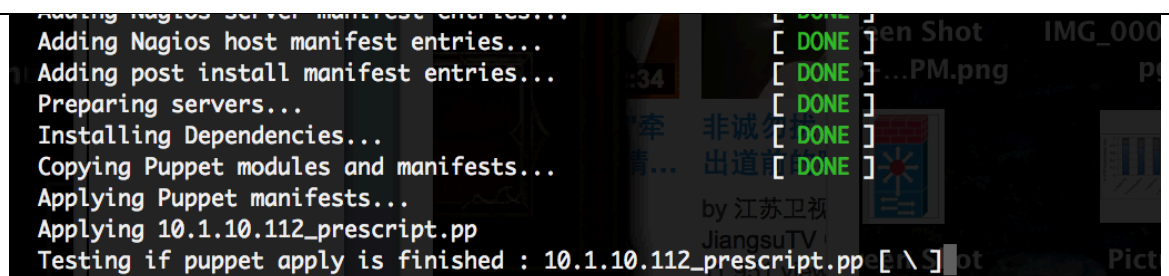
```
# packstack --allinone --provision-demo=n
```



```
[root@s112 ~]# packstack --allinone --provision-demo=n
Welcome to Installer setup utility
Packstack changed given value  to required value /root/.ssh/id_rsa.pub

Installing:
Clean Up... [ DONE ]
Setting up ssh keys...root@10.1.10.112's password: [ DONE ]
Discovering hosts' details... [ DONE ]
Adding pre install manifest entries... [ DONE ]
```

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



```
Adding Nagios server manifest entries... [ DONE ]
Adding Nagios host manifest entries... [ DONE ]
Adding post install manifest entries... [ DONE ]
Preparing servers... [ DONE ]
Installing Dependencies... [ DONE ]
Copying Puppet modules and manifests... [ DONE ]
Applying Puppet manifests... [ DONE ]
Applying 10.1.10.112_prescript.pp
Testing if puppet apply is finished : 10.1.10.112_prescript.pp [ \ ]
```

If everything goes well, you will see this

```
Applying 10.1.10.112-postscript.pp : [ DONE ] 16:44
10.1.10.112-postscript.pp : [ DONE ]
Finalizing... [ DONE ]

**** Installation completed successfully ****

Additional information:
* A new answerfile was created in: /root/packstack-answers-20140222-174026.txt
* Time synchronization installation was skipped. Please note that unsynchronized time 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 directory.
* To use Nagios, browse to http://10.1.10.112/nagios username : nagiosadmin, password : 97ee3888e62440a9
```

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 hypervisor 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
```

Create An Image

Name *

Description

Image Source *

Image Location

Image Location

Format *

QCOW2 - QEMU Emulator

Description:

Specify an image to upload to the Image Service

Currently only images available via an HTTP URL supported. The image location must be accessible to the Image Service. Compressed image binaries are supported (.zip and .tar.gz.)

Please note: The Image Location field MUST be a valid and direct URL to the image binary. URLs that redirect or serve error pages will result in unusable images.

4.3 Create public, private networks, and router

4.3.1 Create public network

Create Network

Name

Project *

admin

Admin State

☒

Shared

☒

External Network

☒

Description:

Select a name for your network.

Cancel

Create Network

4.3.2 Create subnet on the public network

Update Subnet

Subnet *

Subnet Detail

Subnet Name

public 10.1.10.195

Network Address

10.1.10.0/24

Gateway IP (optional)

10.1.10.1

Disable Gateway

☐

You can update a subnet associated with the network. Advanced configuration are available at "Subnet Detail" tab.

Cancel

Update

4.3.3 Subnet detail

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

Create Subnet

Subnet *

Subnet Detail

Enable DHCP

☐

Allocation Pools

10.1.10.195,10.1.10.199

DNS Name Servers

75.75.75.75

Host Routes

You can specify additional attributes for the subnet.

IP address list of DNS name servers for this subnet. One entry per line.

4.3.4 Private network

4.3.4.1 Create private network

The screenshot shows a 'Create Subnet' dialog box with two tabs: 'Subnet *' (active) and 'Subnet Detail'. The 'Subnet *' tab contains the following fields:

- Subnet Name:** A text input field containing '192.168.1.10'.
- Network Address:** A text input field containing '192.168.1.0/24'.
- IP Version *:** A dropdown menu with 'IPv4' selected.
- Gateway IP:** A text input field containing '192.168.1.1'.
- Disable Gateway:** A checkbox that is currently unchecked.

On the right side of the dialog, there is a text block: 'You can create a subnet associated with the network. Advanced configuration are available at "Subnet Detail" tab.'

A tooltip is displayed over the 'Gateway IP' field with the following text: 'IP address of Gateway (e.g. 192.168.0.254) The default value is the first IP of the network address (e.g. 192.168.0.1 for 192.168.0.0/24). If you use the default, leave blank. If you want to use no gateway, check "Disable Gateway" below.'

At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Create'.

4.3.4.2 Subnet detail

For private, you need to enable DHCP.

Create Subnet

Subnet *

Subnet Detail

Enable DHCP

☒

Allocation Pools

DNS Name Servers

75.75.75.75

Host Routes

You can specify additional attributes for the subnet.

IP address list of DNS name servers for this subnet. One entry per line.

Cancel

Create

4.3.5 Create router

Set the router gateway to the public network

Set Gateway

External Network *

public

Router Name *

router

Router ID *

58df2094-3310-49d8-b71c-794acabbbbf5

Description:

You can connect a specified external network to the router. The external network is regarded as a default route of the router and the router acts as a gateway for external connectivity.

Cancel

Set Gateway

Attach the private network to the router, as its interface

Add Interface

Subnet *

private: 192.168.1.0/24 (192.168.1.0)

IP Address (optional)

Router Name *

router

Router ID *

58df2094-3310-49d8-b71c-794acabbbbf5

Description:

You can connect a specified subnet to the router.

The default IP address of the interface created is a gateway of the selected subnet. You can specify another IP address of the interface here. You must select a subnet to which the specified IP address belongs to from the above list.

Cancel

Add 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

Remote *

CIDR

CIDR

0.0.0.0/0

Description:

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

Rule: You can specify the desired rule template use custom rules, the options are Custom TCP Rule, 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 range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports. 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 in this rule.

Enter an integer value between 1 and 65535 for an ICMP type and code in the spaces provided.

Add Rule



Rule *

Custom ICMP Rule

Direction

Ingress

Type

-1

Code

-1

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 ending ports. 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 in this rule.

Enter a value for ICMP code in the range (-1; 255) for ICMP rules you instead specify an ICMP type and code in the spaces provided.

4.5 Launch instance

Launch Instance

Details * Access & Security * Networking * Post-Creation

Availability Zone

nova

Instance Name *

cirros2

Flavor *

m1.tiny

Instance Count *

1

Instance Boot Source *

Boot from image

Image Name

Specify the details for launching an instance.

The chart below shows the resources used by this project in relation to the project's quotas.

Flavor Details

Name	m1.tiny
VCPUs	1
Root Disk	1 GB
Ephemeral Disk	0 GB
Total Disk	1 GB
RAM	512 MB

Project Limits

Number of Instances

1 of 10 Used

Launch Instance

Details * Access & Security * Networking * Post-Creation

Selected Networks

nic:1 private (ce4cde5c-fc71-4348-b125-adc68a6bd228)

Available networks

public (bfea6d29-eb13-4d3f-8cd4-e1687108b2ea)

Choose network from Available networks to Selected Networks by push button or drag and drop, you may change nic order by drag and drop as well.

Cancel

Launch

Now associate a floating IP to the VM

Manage Floating IP Associations

IP Address *

IP Address *

10.1.10.187

+

Port to be associated *

cirros2: 172.16.1.4

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

Cancel

Associate

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”.

```
Connection to 10.1.10.186 closed.
Hui-Kangs-MacBook-Pro-2:~ hkang_sunysb$ ssh cirros@10.1.10.187
^C
Hui-Kangs-MacBook-Pro-2:~ hkang_sunysb$ ssh cirros@10.1.10.187
The authenticity of host '10.1.10.187 (10.1.10.187)' can't be established.
RSA key fingerprint is 11:0f:cf:ed:65:f4:73:98:a3:98:ce:c6:49:22:8d:7f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.10.187' (RSA) to the list of known hosts.
cirros@10.1.10.187's password:
Permission denied, please try again.
cirros@10.1.10.187's password:
Permission denied, please try again.
cirros@10.1.10.187's password:
$
```

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/>