



OpenStack Setup using Horizon - 2

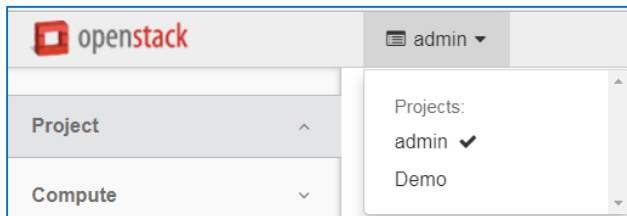
James Won-Ki Hong, Seyeon Jeong, Jian Li

**Dept. of Computer Science & Engineering
POSTECH**

<http://dpm.postech.ac.kr/~jwkhong>
jwkhong@postech.ac.kr

❖ Tenant Network (Demo)

- Private network for an OpenStack tenant
- Logically isolated from other tenants
- Network → Networks → Create Network
- Subnet
 - Network Address: any CIDR for the private network
 - Gateway IP: blank or the first IP of the subnet address
- Subnet Details
 - Enable DHCP
 - Allocation pools for tenant VMs



<Project Change>

Create Network

Network

Subnet

Subnet Details

Subnet Name

tenant1_subnet

Network Address ?

10.10.0.0/24

IP Version

IPv4

Gateway IP ?

10.10.0.1

☐ Disable Gateway

Creates a subnet associated with the network. You need to enter a valid "Network Address" and "Gateway IP". If you did not enter the "Gateway IP", the first value of a network will be assigned by default. If you do not want gateway please check the "Disable Gateway" checkbox. Advanced configuration is available by clicking on the "Subnet Details" tab.

Cancel

« Back

Next »

Create Network

Network

Subnet

Subnet Details

☒ Enable DHCP

Specify additional attributes for the subnet.

Allocation Pools ?

10.10.0.100,10.10.0.150

DNS Name Servers ?

8.8.8.8

Host Routes ?

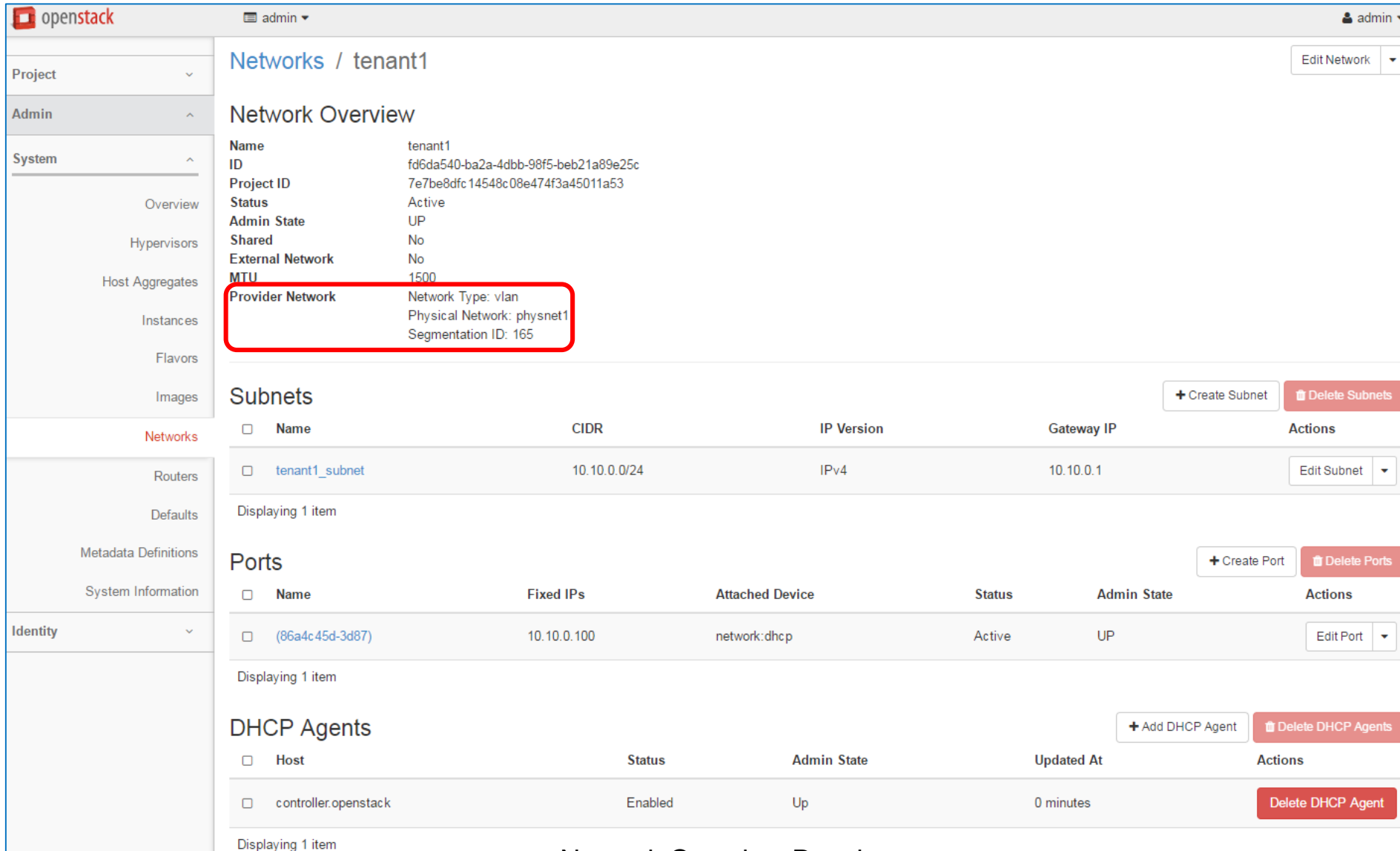
<Tenant Network Setup>

Cancel

« Back

Create

OpenStack Setup using Horizon



The screenshot shows the OpenStack Horizon interface for the 'tenant1' project. The left sidebar contains navigation links for Project, Admin, System, Overview, Hypervisors, Host Aggregates, Instances, Flavors, Images, Networks (highlighted), Routers, Defaults, Metadata Definitions, System Information, Identity, and a user profile dropdown. The main content area is titled 'Networks / tenant1' and includes an 'Edit Network' button. The 'Network Overview' section displays a table of network details for 'tenant1', with the 'Provider Network' row highlighted by a red box. Below this are sections for 'Subnets', 'Ports', and 'DHCP Agents', each with a table of resources and action buttons.

Network Overview

Property	Value
Name	tenant1
ID	fd6da540-ba2a-4dbb-98f5-beb21a89e25c
Project ID	7e7be8dfc14548c08e474f3a45011a53
Status	Active
Admin State	UP
Shared	No
External Network	No
MTU	1500
Provider Network	Network Type: vlan Physical Network: physnet1 Segmentation ID: 165

Subnets

Name	CIDR	IP Version	Gateway IP	Actions
tenant1_subnet	10.10.0.0/24	IPv4	10.10.0.1	Edit Subnet

Displaying 1 item

Ports

Name	Fixed IPs	Attached Device	Status	Admin State	Actions
(86a4c45d-3d87)	10.10.0.100	network:dhcp	Active	UP	Edit Port

Displaying 1 item

DHCP Agents

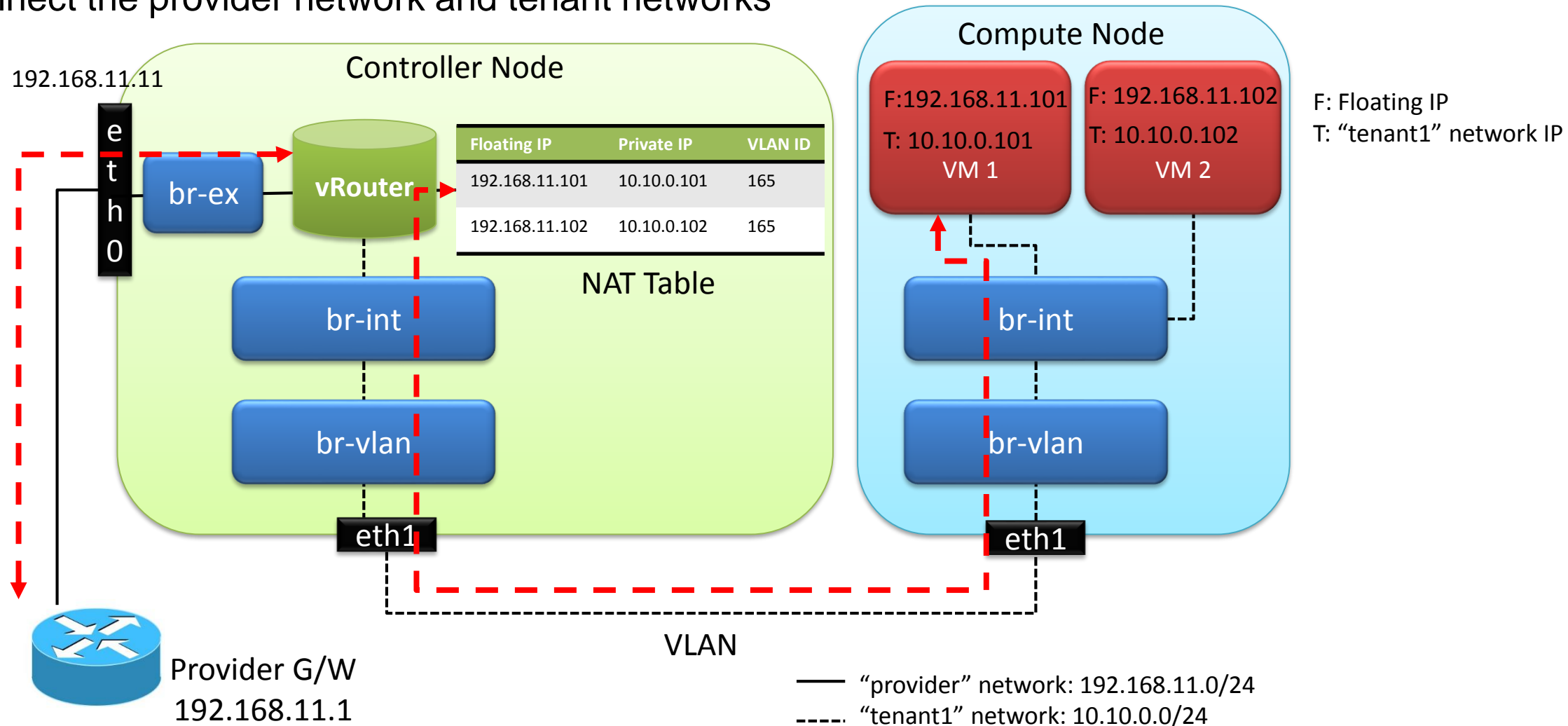
Host	Status	Admin State	Updated At	Actions
controller.openstack	Enabled	Up	0 minutes	Delete DHCP Agent

Displaying 1 item

<Network Overview Panel>

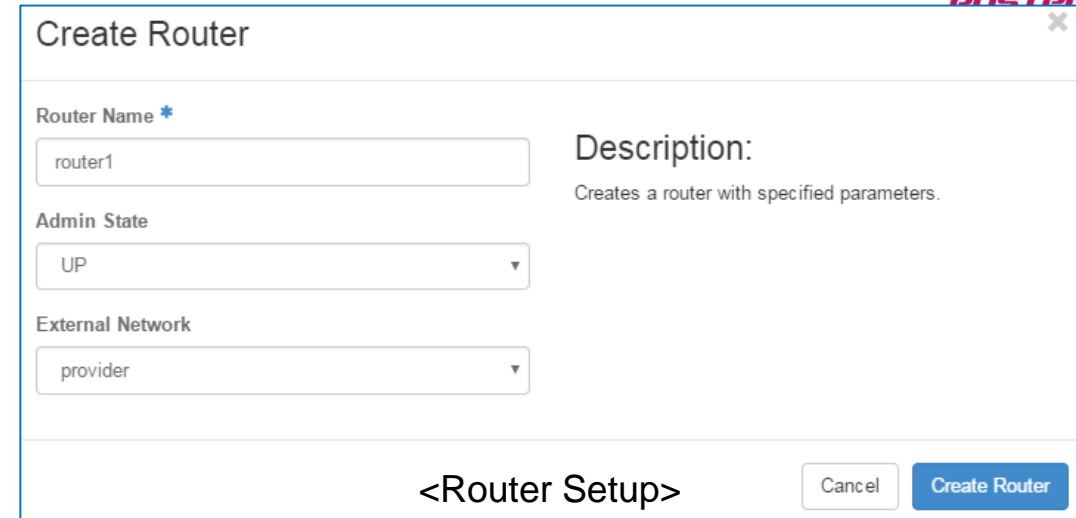
❖ Virtual Router

- Connect the provider network and tenant networks



❖ Virtual Router (Demo)

- Includes a NAT table for translation between a floating IP and private IP of given VM
- Implemented by Neutron L3 agent
- Network → Routers → Create Router
- External Network
 - Select the provider network
- Select “router1” → Interfaces → Add Interface
 - Add an interface for the tenant network to the router created
 - Subnet: tenant1
 - IP address: tenant network’s G/W



Create Router

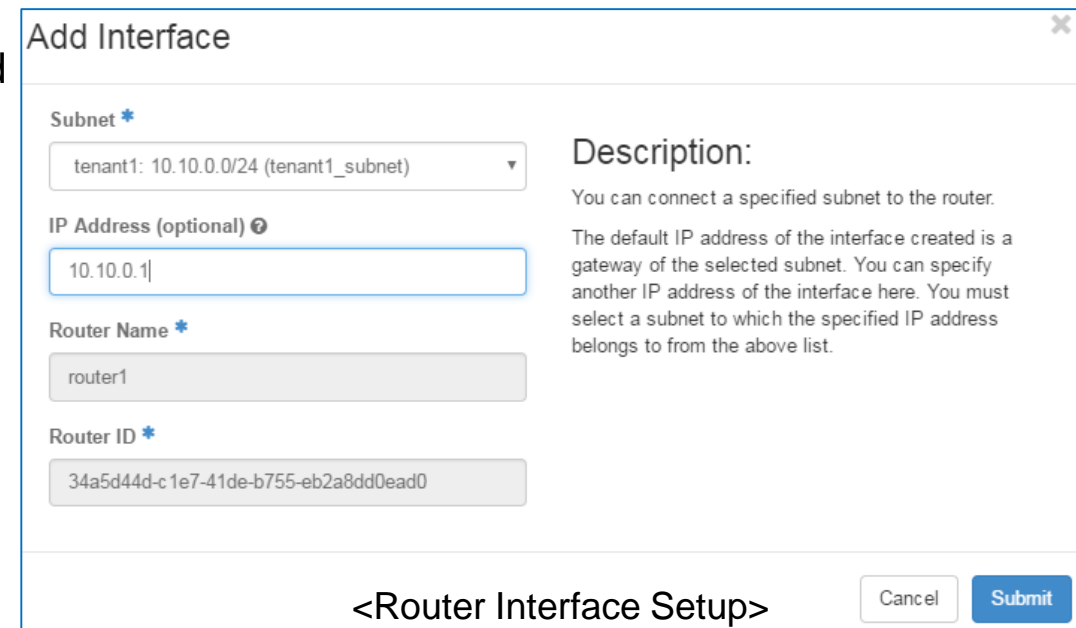
Router Name *
router1

Admin State
UP

External Network
provider

Description:
Creates a router with specified parameters.

<Router Setup> Cancel Create Router



Add Interface

Subnet *
tenant1: 10.10.0.0/24 (tenant1_subnet)

IP Address (optional) ?
10.10.0.1

Router Name *
router1

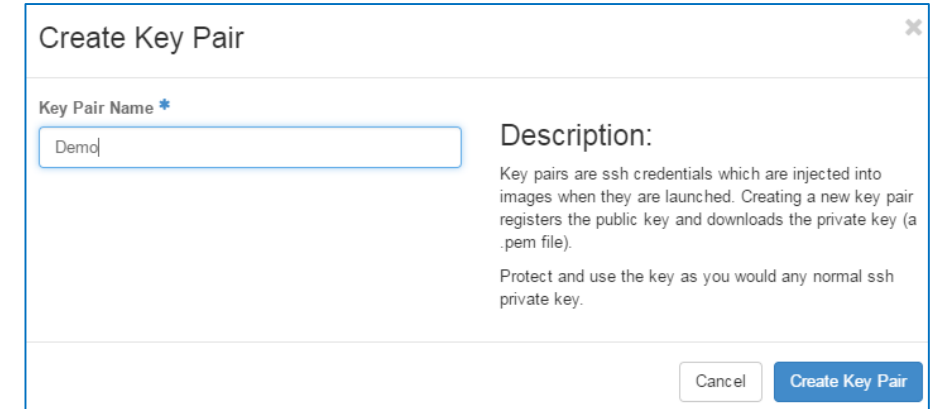
Router ID *
34a5d44d-c1e7-41de-b755-eb2a8dd0ead0

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.

<Router Interface Setup> Cancel Submit

❖ Key Pairs (Demo)

- Needed for SSH connection to tenant's VM instances
 - Generally, OS images for cloud VM don't have a default or common user account to avoid security issues
- Save the public key in Keystone
- Put the downloaded private key in a client machine
- Compute → Access & Security → Key Pairs → Create Key Pair



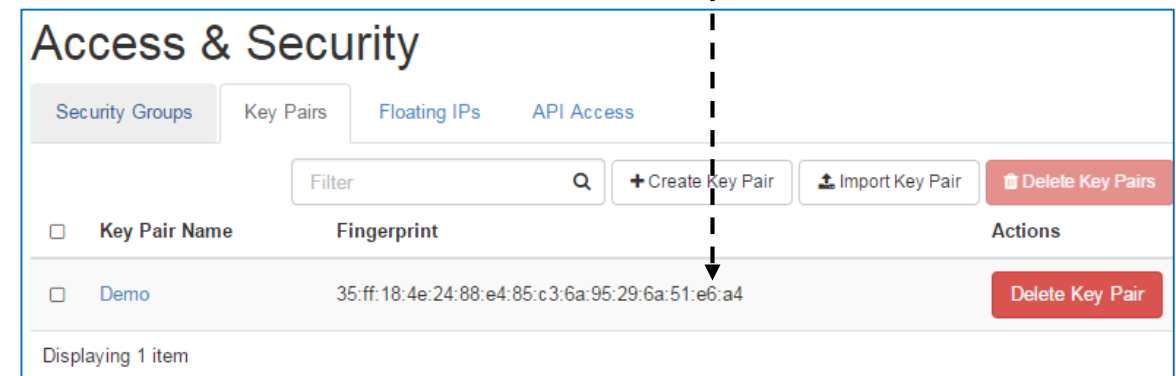
Create Key Pair

Key Pair Name *
Demo

Description:
Key pairs are ssh credentials which are injected into images when they are launched. Creating a new key pair registers the public key and downloads the private key (a .pem file).
Protect and use the key as you would any normal ssh private key.

Cancel Create Key Pair

<Key Pair Setup>



Access & Security

Security Groups Key Pairs Floating IPs API Access

Filter + Create Key Pair Import Key Pair Delete Key Pairs

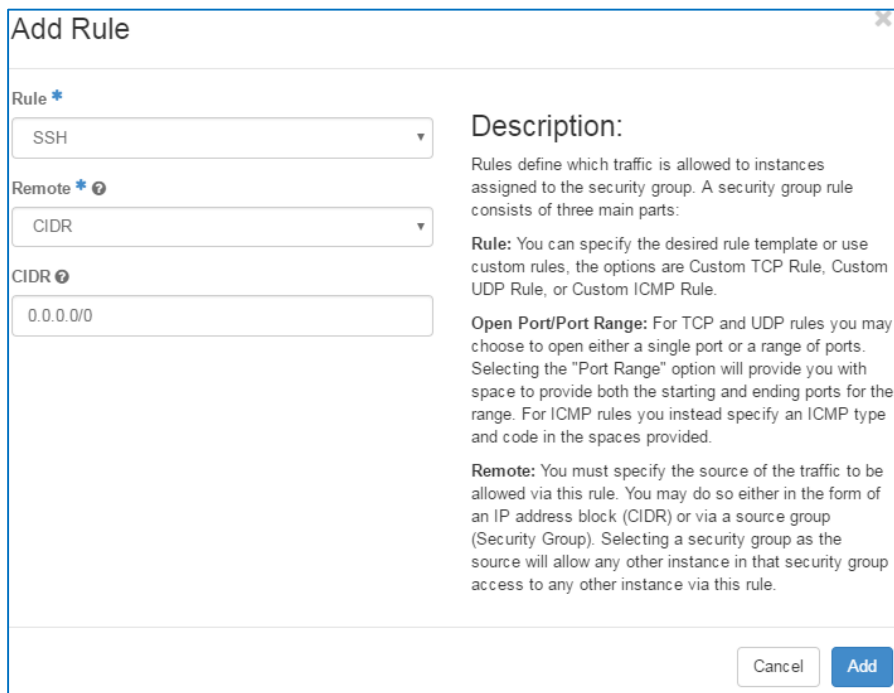
<input type="checkbox"/>	Key Pair Name	Fingerprint	Actions
<input type="checkbox"/>	Demo	35:ff:18:4e:24:88:e4:85:c3:6a:95:29:6a:51:e6:a4	Delete Key Pair

Displaying 1 item

<Access & Security Panel>

❖ Security Groups (Demo)

- Tenant-level firewall rules
- Each VM instance can have a different Security Group
- Compute → Access & Security → Security Groups → Manage rules for “default” Security Group → Add Rule
- Permit ingress/egress ALL ICMP and SSH traffic



Add Rule

Rule *
SSH

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:

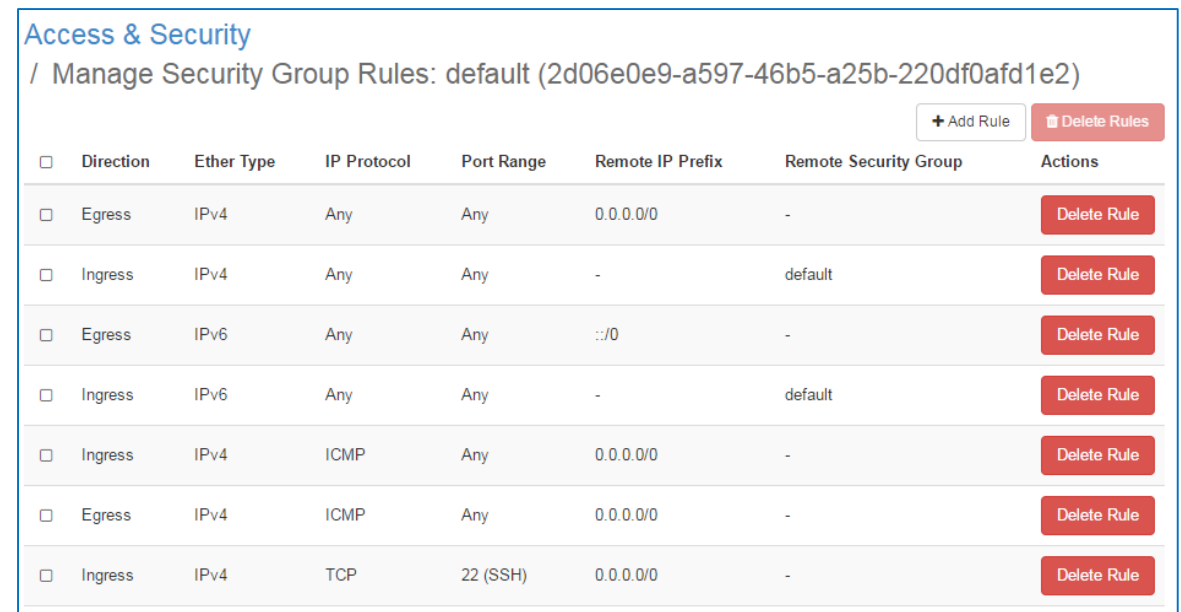
Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

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

<Firewall Rule Setup>



Access & Security
/ Manage Security Group Rules: default (2d06e0e9-a597-46b5-a25b-220df0afd1e2)

+ Add Rule Delete Rules

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	Any	Any	-	default	Delete Rule
<input type="checkbox"/>	Egress	IPv6	Any	Any	:::/0	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv6	Any	Any	-	default	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	Delete Rule
<input type="checkbox"/>	Egress	IPv4	ICMP	Any	0.0.0.0/0	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	Delete Rule

<Security Groups Panel>

Project ^

Compute ^

Overview

Instances

Images

Access & Security

Network v

Admin v

Identity v

Instances

Instance Name =

Filter

Launch Instance

Instance Name

Image Name

IP Address

Size

Key Pair

Status

Availability Zone

Task

Power State

Time since created

Actions

No items to display.