OpenStack Labs

Lab 04: Deploying an External Instance

Contents

About This Document

- This document was developed by a team at the University of Tennessee at Chattanooga led by Dr. Mengjun Xie (**mengjun-xie@utc.edu**).
- The development of this document was supported by a National Centers of Academic Excellence in Cybersecurity Grant (#H98230-20-1-0351), housed at the National Security Agency.
-

Introduction

Up to this point, everything you have worked on has been local to the OpenStack environment. In this lab, you will learn the various concepts necessary to give OpenStack instances and networks external connectivity. You will manage external networks, routers, and floating IP addresses to give OpenStack instances and networks external connectivity; SSH key pairs to allow you to connect to an OpenStack instance from outside the OpenStack environment; and security groups to prevent unwanted traffic in the network. These resources will come together to allow OpenStack instances to provide services outside the OpenStack cloud and allow you to manage instances from outside the cloud.

Objectives

- Create and manage external networks.
- Create and manage OpenStack routers.
- Create and manage floating IP addresses.
- Create and manage SSH key pairs.
- Create and manage security groups.
- Launch and verify an external instance.

Lab Settings

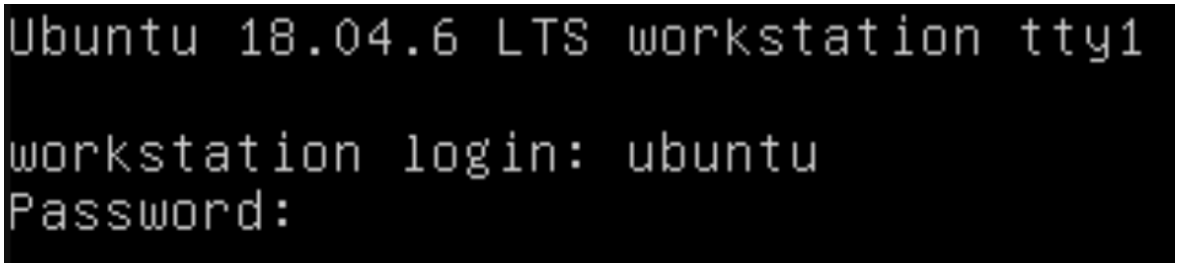
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account	Password
workstation	ens3: 192.168.1.21 ens4: 172.25.250.21	ubuntu	ubuntu
devstack	ens3: 192.168.20 ens4: 172.25.250.20	ubuntu	ubuntu

1 Managing External Networks

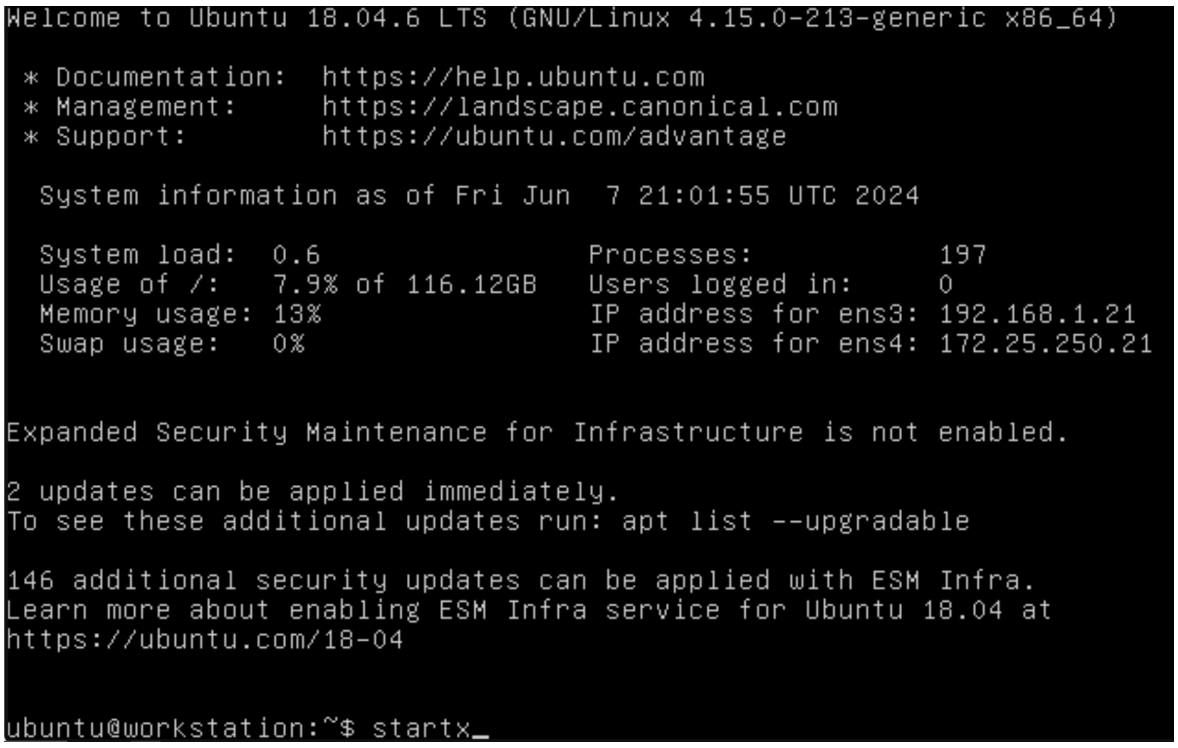
In this task, you will use the *Horizon Dashboard* and the **OpenStack Unified CLI** to create and configure an external network.

1.1. Log into the **workstation** machine as the **ubuntu** user with password **ubuntu**.



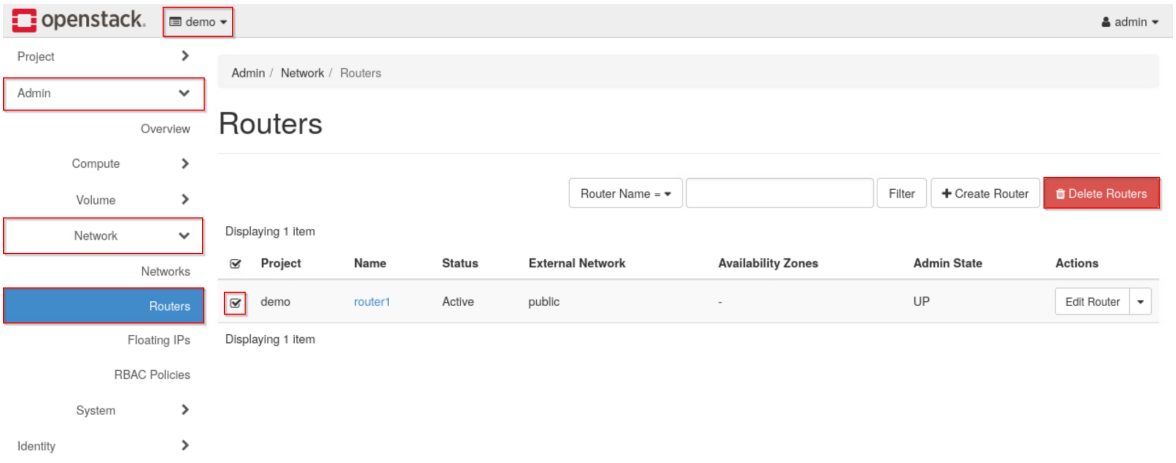
1.2. Launch the graphical user interface.

```
ubuntu@workstation:~$ startx
```

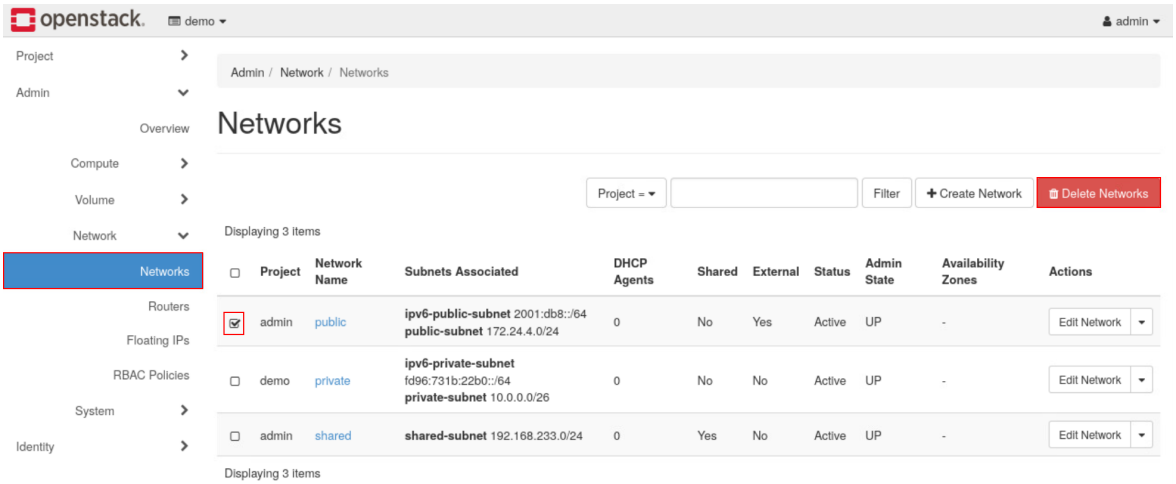


1.3. Open the web browser. Navigate to **192.168.1.20** and log in to the dashboard as **admin** with the password **secret**. In this lab, we will create our own public network and router. The **demo** project already has a default router and public network, so those need to be deleted first.

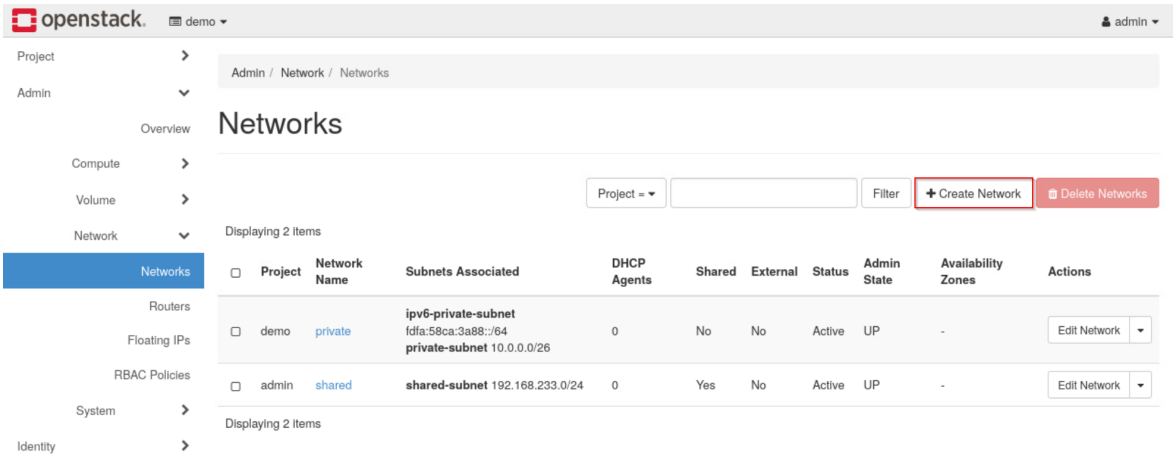
1.4. Switch to the **demo** project. Navigate to **Admin** > **Network** > **Routers**. Check the box in the same row as **router1**, then click **Delete Routers**.



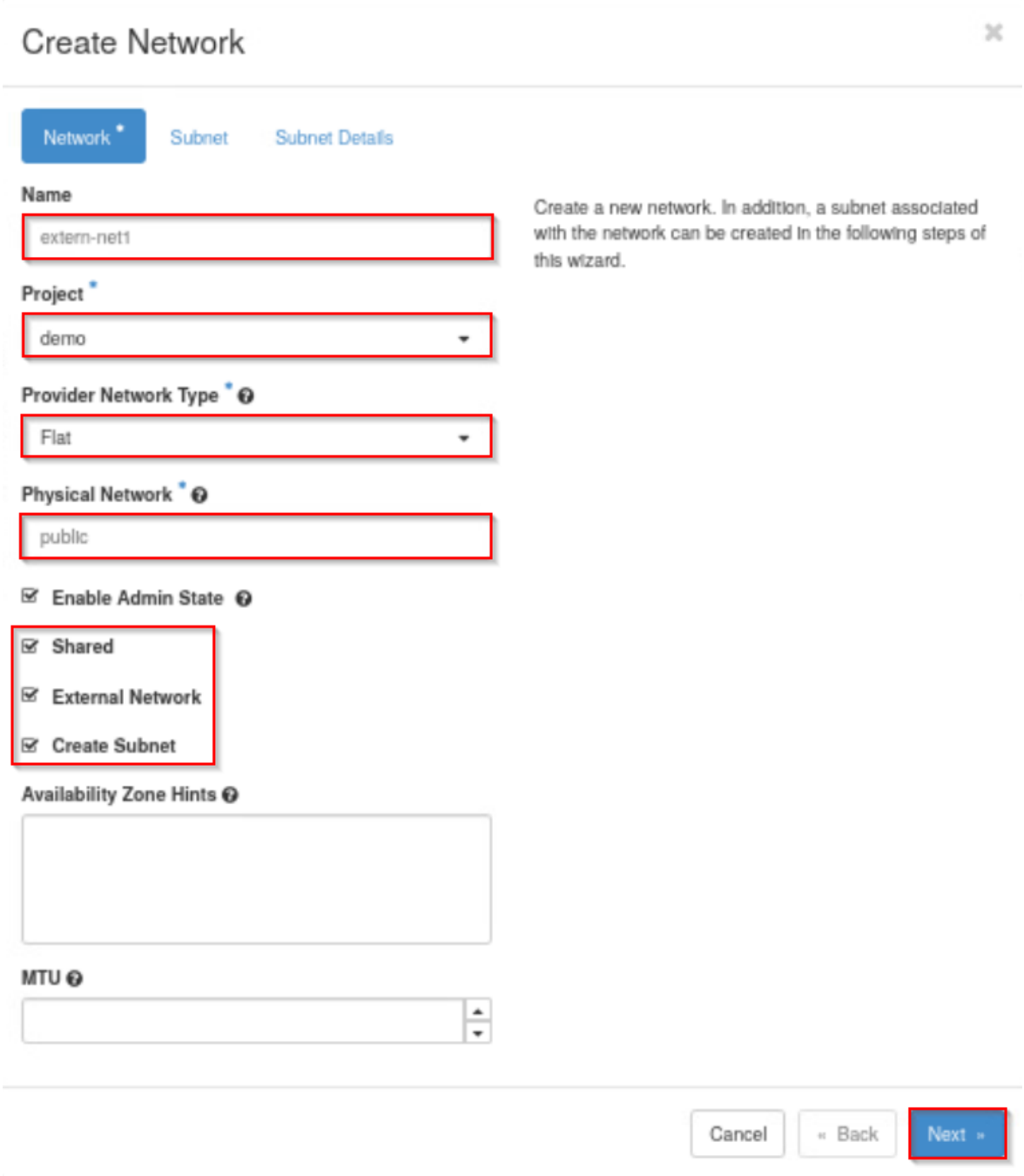
1.5. Now, navigate to **Networks**. Check the box in the same row as **public**, then click **Delete Networks**.



1.6. Click **Create Network**.



1.7. Enter **extern-net1** in the *Network Name* field. Select **demo** in the *Project* dropdown. For *Provider Network Type*, select **Flat**. Enter **public** into the *Physical Network* field. Check the *Shared* and *External Network* check boxes, and ensure the *Create Subnet* check box is checked. Click **Next** to go to the *Subnet* tab.

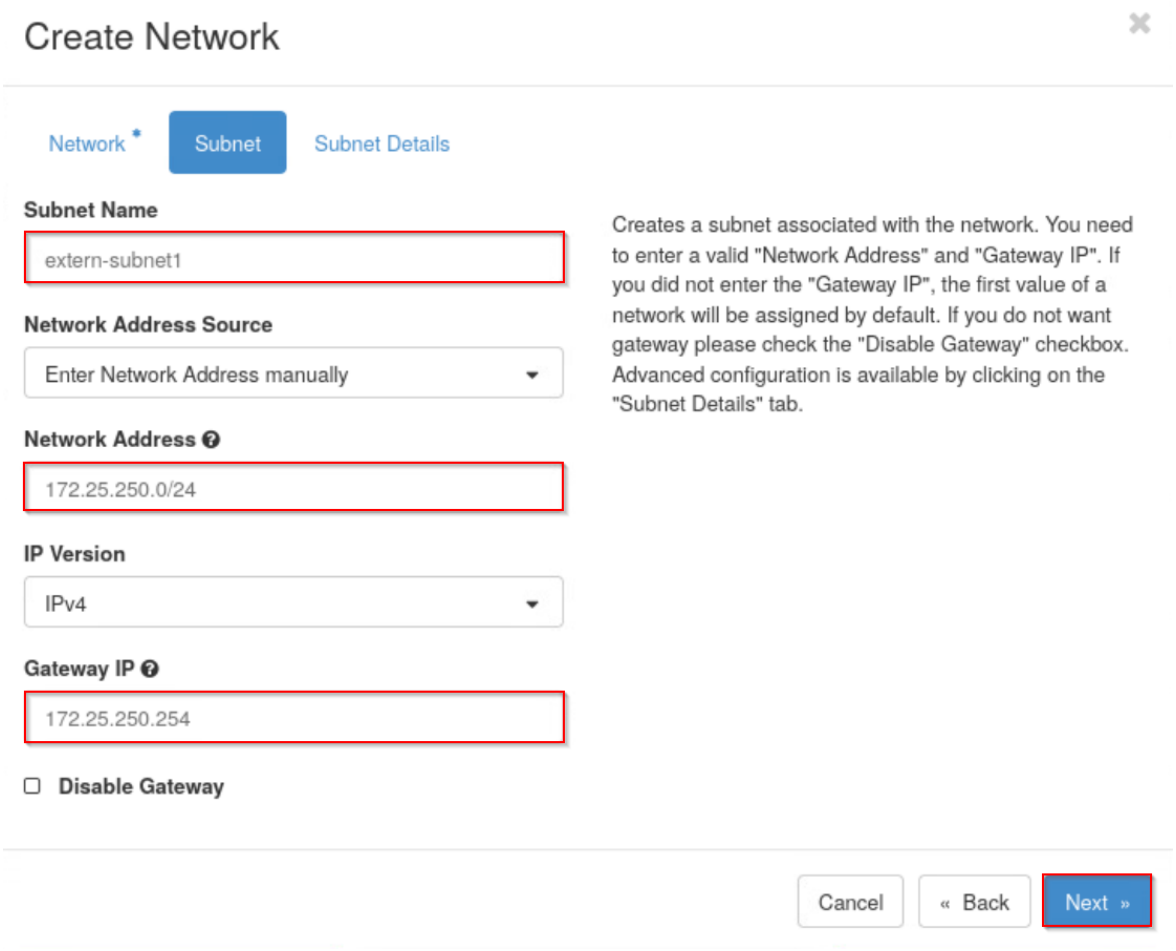


Note

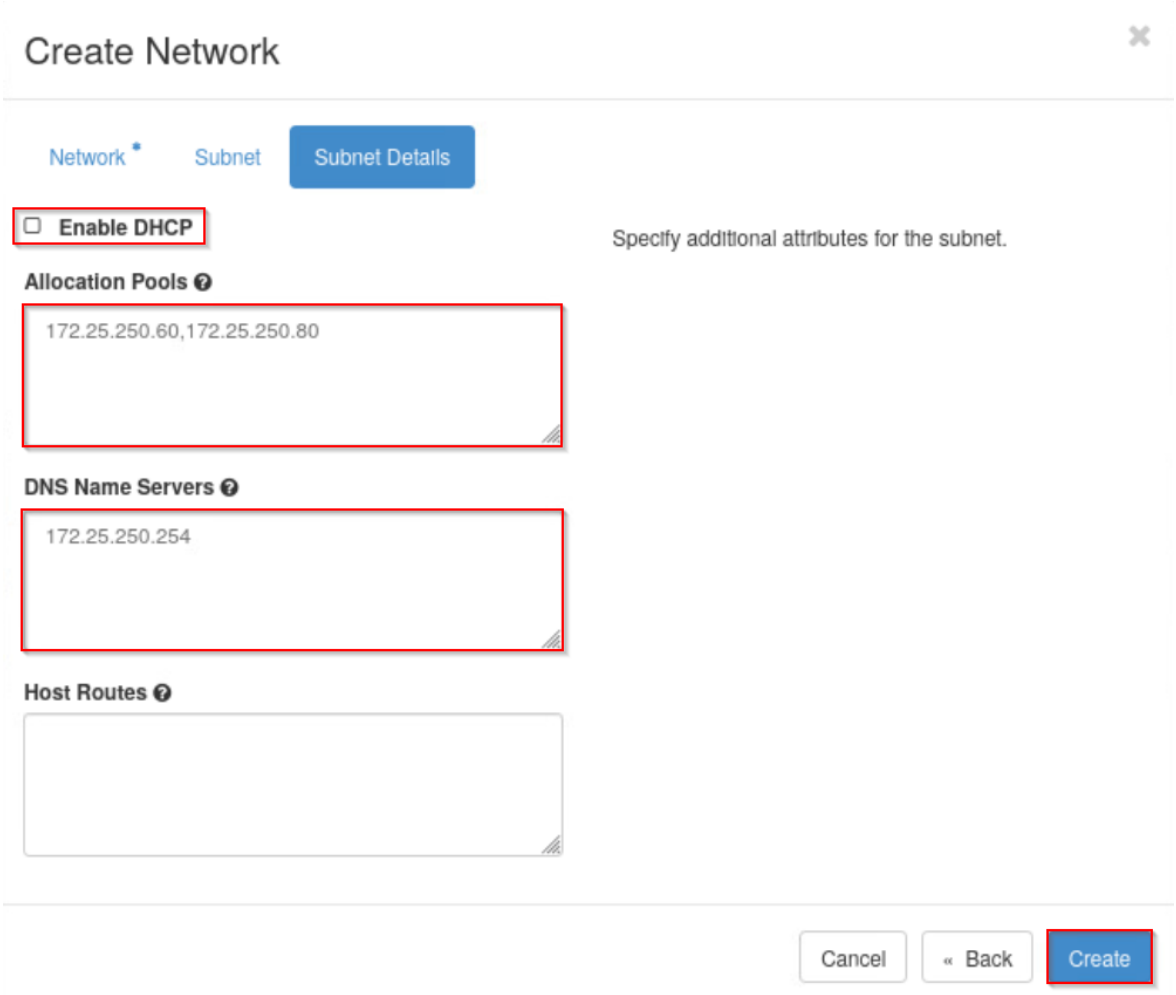
The **public** physical network is different from the **public** network we just deleted. This physical network is the name assigned to the physical or provider network that OpenStack uses for external communication. This resource did not get deleted with

the network of the same name since they are independent. The **public** network that was deleted was a virtual network implemented on top of the physical network.

1.8. In the *Subnet* tab, enter **extern-subnet1** in the *Subnet Name* field, enter **172.25.250.0/24** in the *Network Address* field, and enter **172.25.250.254** in the *Gateway IP* field. Click **Next** to go to the *Subnet Details* tab.



1.9. In the *Subnet Details* tab, uncheck the *Enable DHCP* check box since we want to assign static IP addresses on this network. Enter **172.25.250.60, 172.25.250.80** in the *Allocation Pools* field so that any IP address allocated for this network will fall in this range of addresses. Enter **172.25.250.254** in the *DNS Name Servers* field. Click **Create** to create the network and subnet.



1.10. Log out of the *Horizon Dashboard* and close the web browser.

1.11. Open a terminal window and source the keystone credentials for the **admin** user.

```
ubuntu@workstation:~$ source ~/keystonerc-admin
```

1.12. List the available networks.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list \
> --max-width 100
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list \
> --max-width 100
+--------------------------------------+------------+--------------------------------------+
| ID                                   | Name       | Subnets                              |
+--------------------------------------+------------+--------------------------------------+
| 966ecb4f-4ff8-44ea-a476-2d2f18955085 | private    | 674205b6-1357-4727-a21a-94220492a57f,|
|                                      |            | fa8a2545-5a8c-44a2-bacc-1b86c253b880 |
| 9f23266f-d833-4337-9a27-4818a6d28e9e | shared     | 7e456257-76e5-4cfc-bf3f-b2a3876dba40 |
| d4c0e1c8-0cb5-4e1c-90b1-3f9a3b392e88 | extern-net1| 93a361f0-2637-4e7d-b41c-88fa0209350b |
+--------------------------------------+------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

When typing the command, make sure there is a space between **extern-net2** and the \ character, and press **Enter** to get the > and continue typing the rest of the command.

Tip

To keep the output from overflowing while keeping the formatting intact, use the **–max-width n** option to limit the output to **n** characters per line. This is especially useful for commands that output long IDs or have many columns in the output table.

1.13. The next set of steps will show how to recreate the external network from the beginning of the lab from the CLI. To free up the necessary resources, first delete the **extern-net1** network. This will also delete the **extern-subnet1** subnet.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network delete extern-net1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network delete extern-net1
[ubuntu@workstation (keystone-admin)]:~$
```

1.14. List the networks again to confirm that **extern-net1** was deleted successfully.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list \
> --max-width 100
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list \
> --max-width 100
+--------------------------------------+---------+--------------------------------------+
| ID                                   | Name    | Subnets                              |
+--------------------------------------+---------+--------------------------------------+
| 966ecb4f-4ff8-44ea-a476-2d2f18955085 | private | 674205b6-1357-4727-a21a-94220492a57f,|
|                                      |         | fa8a2545-5a8c-44a2-bacc-1b86c253b880 |
| 9f23266f-d833-4337-9a27-4818a6d28e9e | shared  | 7e456257-76e5-4cfc-bf3f-b2a3876dba40 |
+--------------------------------------+---------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

1.15. Create an external network named **extern-net2**. Set the network type to **flat** and the physical network to **public**. Set the network as shared and external.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network create \
> --external --share \
> --provider-network-type flat \
> --provider-physical-network public \
> extern-net2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network create \
> --external --share \
> --provider-network-type flat \
> --provider-physical-network public \
> extern-net2
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | UP                                   |
| availability_zone_hints   |                                      |
| availability_zones        |                                      |
| created_at                | 2024-06-17T18:45:46Z                 |
| description               |                                      |
| dns_domain                | None                                 |
| id                        | d1e72c9b-87be-4b48-aa49-a39b1f232e14 |
| ipv4_address_scope        | None                                 |
| ipv6_address_scope        | None                                 |
| is_default                | False                                |
| is_vlan_transparent       | None                                 |
| mtu                       | 1500                                 |
| name                      | extern-net2                          |
| port_security_enabled     | True                                 |
| project_id                | 39e851b14f864573aad60582c35e40dc     |
| provider:network_type     | flat                                 |
| provider:physical_network | public                               |
| provider:segmentation_id  | None                                 |
| qos_policy_id             | None                                 |
| revision_number           | 1                                    |
| router:external           | External                             |
| segments                  | None                                 |
| shared                    | True                                 |
| status                    | ACTIVE                               |
| subnets                   |                                      |
| tags                      |                                      |
| updated_at                | 2024-06-17T18:45:46Z                 |
+---------------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

1.16. Create a subnet named **extern-subnet2** in the **extern-net2** network. Give the subnet a range of **172.25.250.60** to **172.25.250.80**. Disable DHCP services for the subnet and use the address **172.25.250.254** as the gateway as well as the DNS name server.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack subnet create \
> --subnet-range 172.25.250.0/24 \
> --no-dhcp \
> --gateway 172.25.250.254 \
> --dns-nameserver 172.25.250.254 \
> --allocation-pool start=172.25.250.60,end=172.25.250.80 \
> --network extern-net2 \
> extern-subnet2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack subnet create \
> --subnet-range 172.25.250.0/24 \
> --no-dhcp \
> --gateway 172.25.250.254 \
> --dns-nameserver 172.25.250.254 \
> --allocation-pool start=172.25.250.60,end=172.25.250.80 \
> --network extern-net2 \
> extern-subnet2
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| allocation_pools  | 172.25.250.60-172.25.250.80          |
| cidr              | 172.25.250.0/24                      |
| created_at        | 2024-06-17T18:48:22Z                 |
| description       |                                      |
| dns_nameservers   | 172.25.250.254                       |
| enable_dhcp       | False                                |
| gateway_ip        | 172.25.250.254                       |
| host_routes       |                                      |
| id                | 1534a6ca-bde0-4d67-8b6f-1edd4d67b2f1 |
| ip_version        | 4                                    |
| ipv6_address_mode | None                                 |
| ipv6_ra_mode      | None                                 |
| name              | extern-subnet2                       |
| network_id        | d1e72c9b-87be-4b48-aa49-a39b1f232e14 |
| project_id        | 39e851b14f864573aad60582c35e40dc     |
| revision_number   | 0                                    |
| segment_id        | None                                 |
| service_types     |                                      |
| subnetpool_id     | None                                 |
| tags              |                                      |
| updated_at        | 2024-06-17T18:48:22Z                 |
+-------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

1.17. List the networks again to see that **extern-net2** and **extern-subnet2** were created successfully.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list \
> --max-width 100
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list \
> --max-width 100
+--------------------------------------+-------------+--------------------------------------+
| ID                                   | Name        | Subnets                              |
+--------------------------------------+-------------+--------------------------------------+
| 966ecb4f-4ff8-44ea-a476-2d2f18955085 | private     | 674205b6-1357-4727-a21a-94220492a57f,    |
|                                      |             | fa8a2545-5a8c-44a2-bacc-1b86c253b880     |
| 9f23266f-d833-4337-9a27-4818a6d28e9e | shared      | 7e456257-76e5-4cfc-bf3f-b2a3876dba40     |
| d1e72c9b-87be-4b48-aa49-a39b1f232e14 | extern-net2 | 1534a6ca-bde0-4d67-8b6f-1edd4d67b2f1     |
+--------------------------------------+-------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

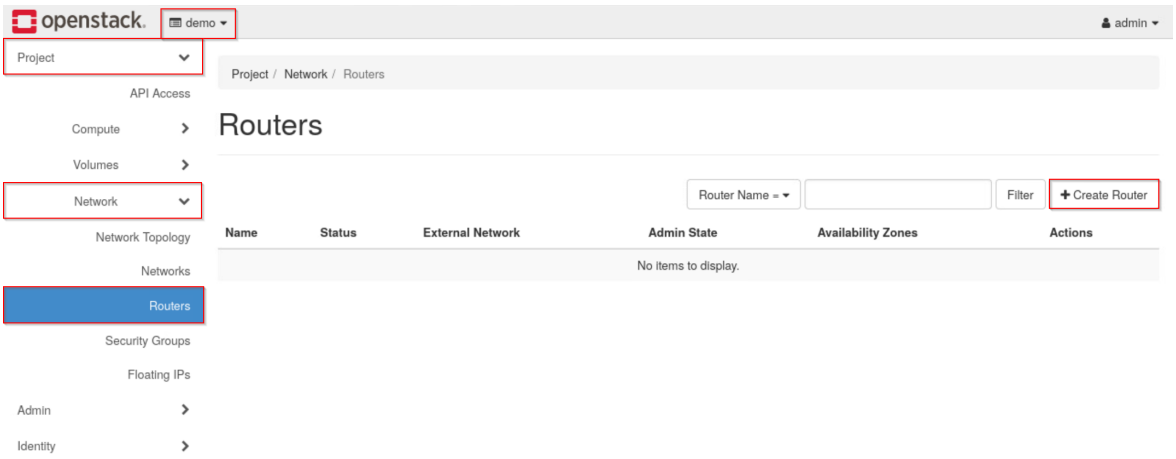
1.18. Leave the terminal window open and continue to the next task.

2 Preparing OpenStack Routers to Deploy an Instance

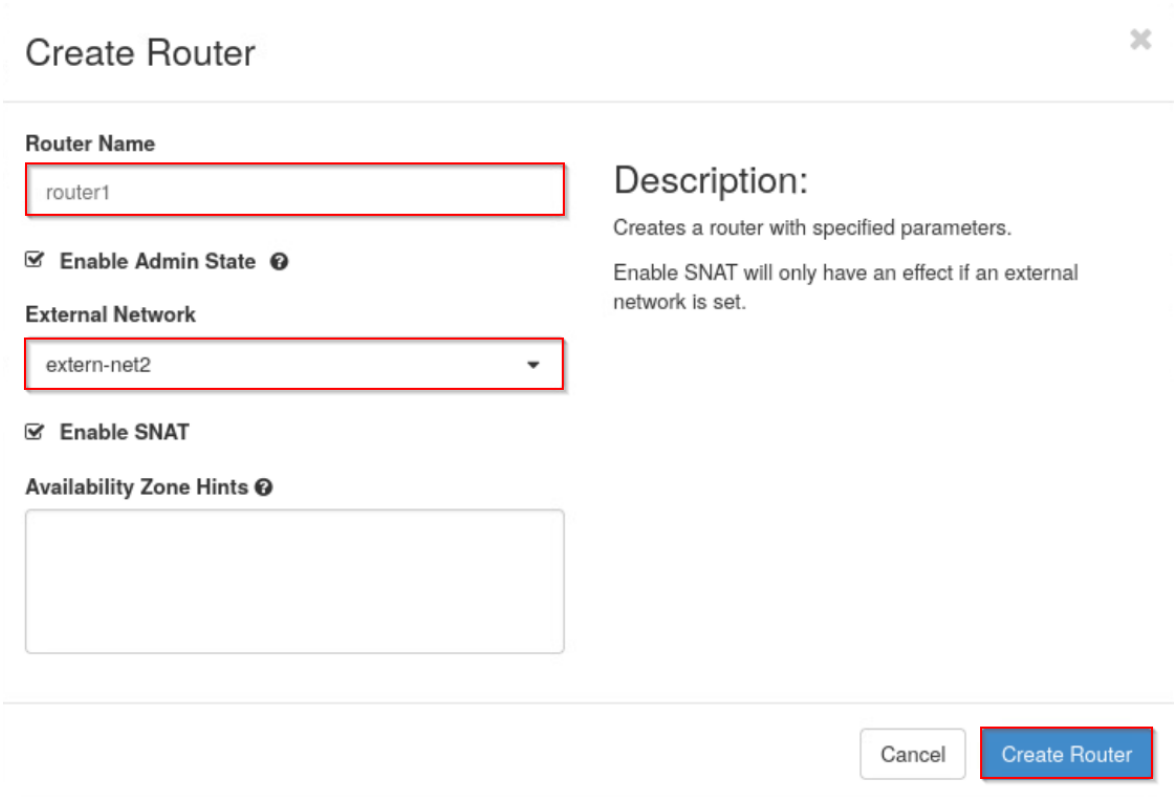
In this task, you will create and configure a router with the *Horizon Dashboard* and *OpenStack CLI* and use command line tools to test the connectivity of the router. The router will serve to connect the external instance to other networks both within OpenStack and outside the cloud.

2.1. Open the web browser and navigate to **192.168.1.20**. Log into the dashboard as **admin** with the password **secret**.

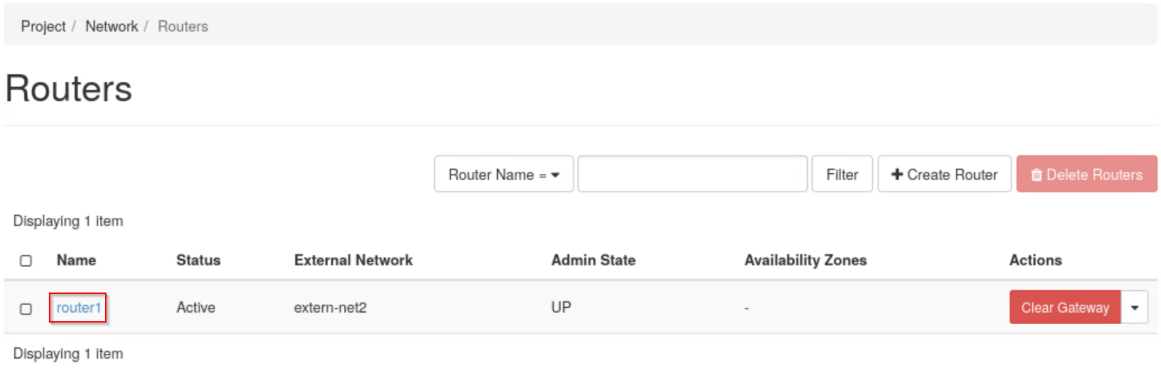
2.2. Switch to the **demo** project and navigate to **Project** > **Network** > **Routers**. Click **Create Router** to create a new router.



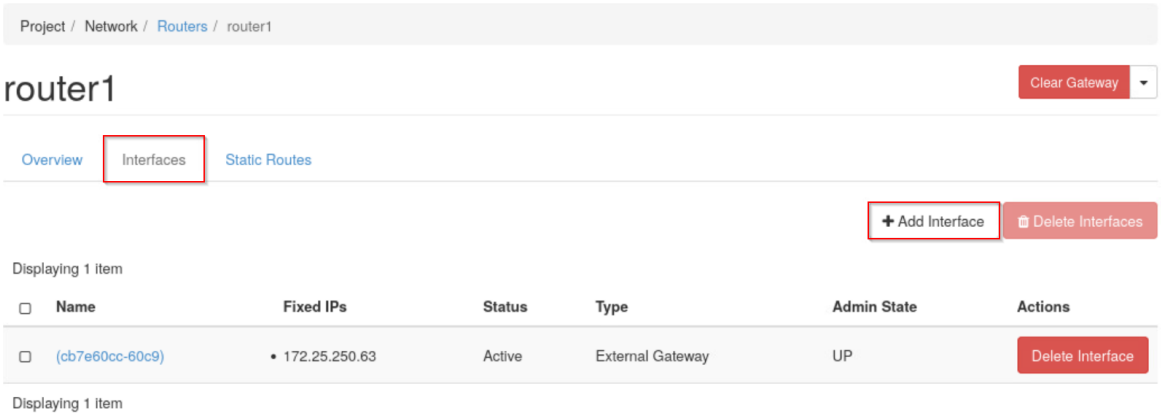
2.3. Enter **router1** in the *Router Name* field and select **extern-net2** in the *External Network* dropdown. Click **Create Router**.



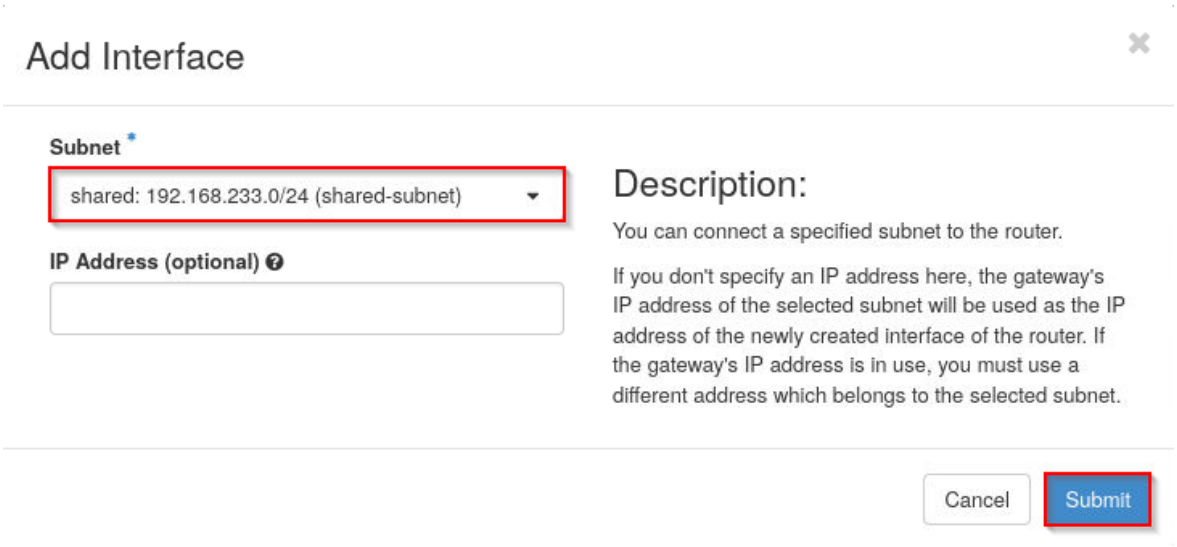
2.4. Click the router name, **router1**, to access its details.



2.5. Click the **Interfaces** tab to manage the interfaces for the router. Notice that currently, the router only has an interface connecting it to the **extern-net2** external network. This will connect instances on this network to networks outside the cloud. We will add an interface to connect **extern-net2** to another network within the OpenStack cloud environment. Click **Add Interface** to add a new interface.



2.6. Select **shared: 192.168.233.0/24 (shared-subnet)** from the *Subnet* dropdown and click **Submit** to add the interface. This will connect the **extern-net2** network to the **shared** network.



Tip

You can delete an interface by selecting the checkbox next to the interface name, then clicking **Delete Interfaces**. Alternatively, simply click **Delete Interface** in the same row as the target interface.

2.7. Log out of the dashboard and close the web browser.

2.8. Open a terminal window if one is not already open, and source the **admin** credentials.

```
ubuntu@workstation:~$ source ~/keystonerc-admin
```

```
ubuntu@workstation:~$ source ~/keystonerc-admin
[ubuntu@workstation (keystone-admin)]:~$
```

2.9. Next, we will recreate this router from the CLI, so we will delete **router1**. First, however, we will see how to remove subnets and gateways from the router. Recall that in a previous step, we added an interface to connect **router1** to the **shared-subnet** subnet on the **shared** network. Remove the connection to this subnet.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router remove subnet \
> router1 \
> shared-subnet
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router remove subnet \
> router1 \
> shared-subnet
[ubuntu@workstation (keystone-admin)]:~$
```

2.10. Unset the **extern-net2** network as the gateway for the router.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router unset \
> --external-gateway router1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router unset \
> --external-gateway router1
[ubuntu@workstation (keystone-admin)]:~$
```

2.11. Delete the **router1** router.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router delete router1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router delete router1
[ubuntu@workstation (keystone-admin)]:~$
```

> **Note**
>
> Deleting a router will also delete its associated interfaces, subnets, and gateways. The previous steps that performed these steps manually were only for demonstration and are not necessary for simply deleting the router.

2.12. Now, we will replicate the previous router from the CLI. Create a router named **router2**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router create router2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router create router2
+-------------------------+--------------------------------------+
| Field                   | Value                                |
+-------------------------+--------------------------------------+
| admin_state_up          | UP                                   |
| availability_zone_hints |                                      |
| availability_zones      |                                      |
| created_at              | 2024-06-17T21:13:43Z                 |
| description             |                                      |
| distributed             | False                                |
| external_gateway_info   | None                                 |
| flavor_id               | None                                 |
| ha                      | False                                |
| id                      | 2ec1b86d-a3ab-4c41-a1c9-af0b006270b3 |
| name                    | router2                              |
| project_id              | 39e851b14f864573aad60582c35e40dc     |
| revision_number         | 1                                    |
| routes                  |                                      |
| status                  | ACTIVE                               |
| tags                    |                                      |
| updated_at              | 2024-06-17T21:13:43Z                 |
+-------------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

2.13. Connect the router to the **shared-subnet** subnet.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router add subnet \
> router2 \
> shared-subnet
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router add subnet \
> router2 \
> shared-subnet
[ubuntu@workstation (keystone-admin)]:~$
```

2.14. Set the **extern-net2** network as the gateway for the router.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router set \
> --external-gateway extern-net2 \
> router2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router set \
> --external-gateway extern-net2 \
> router2
[ubuntu@workstation (keystone-admin)]:~$
```

2.15. Show the details of the **router2** router. Take note of the IP address listed in the *external_gateway_info* row, as you will ping this address in a later step to verify that the router can be reached.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router show \
> --max-width 100 router2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router show \
> --max-width 100 router2
+-------------------------+------------------------------------------------------------------------------+
| Field                   | Value                                                                        |
+-------------------------+------------------------------------------------------------------------------+
| admin_state_up          | UP                                                                           |
| availability_zone_hints |                                                                              |
| availability_zones      |                                                                              |
| created_at              | 2024-06-17T21:13:43Z                                                         |
| description             |                                                                              |
| distributed             | False                                                                        |
| external_gateway_info   | {"network_id": "d1e72c9b-87be-4b48-aa49-a39b1f232e14", "enable_snat":         |
|                         | true, "external_fixed_ips": [{"subnet_id": "1534a6ca-bde0-4d67-8b6f-         |
|                         | 1edd4d67b2f1", "ip_address": "172.25.250.79"}]}                              |
| flavor_id               | None                                                                         |
| ha                      | False                                                                        |
| id                      | 2ec1b86d-a3ab-4c41-a1c9-af0b006270b3                                         |
| interfaces_info         | [{"subnet_id": "7e456257-76e5-4cfc-bf3f-b2a3876dba40", "ip_address":         |
|                         | "192.168.233.1", "port_id": "cb077fb5-259e-48b9-a7b4-30d09a87369e"}]         |
| name                    | router2                                                                      |
| project_id              | 39e851b14f864573aad60582c35e40dc                                             |
| revision_number         | 6                                                                            |
| routes                  |                                                                              |
| status                  | ACTIVE                                                                       |
| tags                    |                                                                              |
| updated_at              | 2024-06-17T21:15:52Z                                                         |
+-------------------------+------------------------------------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

2.16. In order to test the connectivity of the router, SSH into the **devstack** virtual machine. Log in with the password **ubuntu**.

```
[ubuntu@workstation (keystone-admin)]:~$ ssh 192.168.1.20
```

```
[ubuntu@workstation (keystone-admin)]:~$ ssh 192.168.1.20
ubuntu@192.168.1.20's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Feb  9 22:37:16 2024
ubuntu@devstack:~$
```

2.17. Use the **ping** command on the IP address found from the **openstack router show** command to verify that the router can be reached. Receiving ping replies verifies the connectivity of the router since the **devstack** machine is outside the OpenStack cloud environment.

```
ubuntu@devstack:~$ ping -c3 172.25.250.79
```

```
ubuntu@devstack:~$ ping -c3 172.25.250.79
PING 172.25.250.79 (172.25.250.79) 56(84) bytes of data.
64 bytes from 172.25.250.79: icmp_seq=1 ttl=254 time=52.8 ms
64 bytes from 172.25.250.79: icmp_seq=2 ttl=254 time=0.587 ms
64 bytes from 172.25.250.79: icmp_seq=3 ttl=254 time=0.577 ms

--- 172.25.250.79 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.577/17.999/52.835/24.632 ms
ubuntu@devstack:~$
```

Note

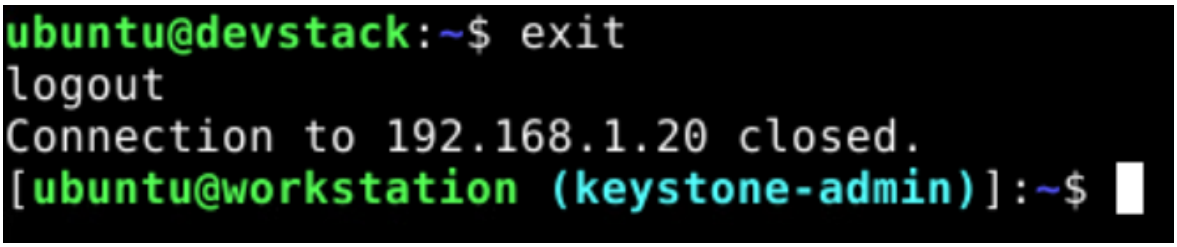
The actual IP address may differ from this example.

Note

You should receive three successful ping replies.

2.18. Exit the SSH session.

```
[ubuntu@workstation (keystone-admin)]:~$ exit
```



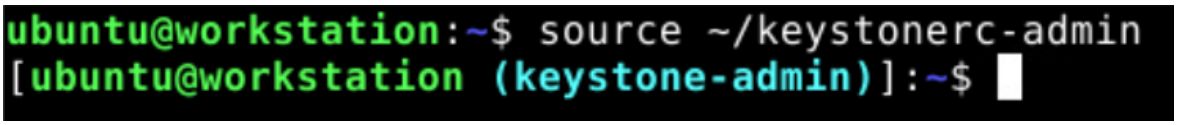
2.19. Leave the terminal window open and continue to the next task.

3 Maintaining Floating IP Addresses

In this task, you will create a floating IP address and allocate it to an instance with the Horizon Dashboard and the OpenStack Unified CLI. While instances are assigned a private, fixed IP address at creation to communicate with other instances, they can also be assigned a floating IP address, which is used for communication outside the OpenStack cloud environment. While the private IP address of instance is fixed until the instance is deleted, a floating IP address can be exchanged for a different one while the instance is still running.

3.1. If a terminal window is not already open, open one and source the admin credentials from the ~**/keystonerc-admin** file.

```
ubuntu@workstation:~$ source ~/keystonerc-admin
```



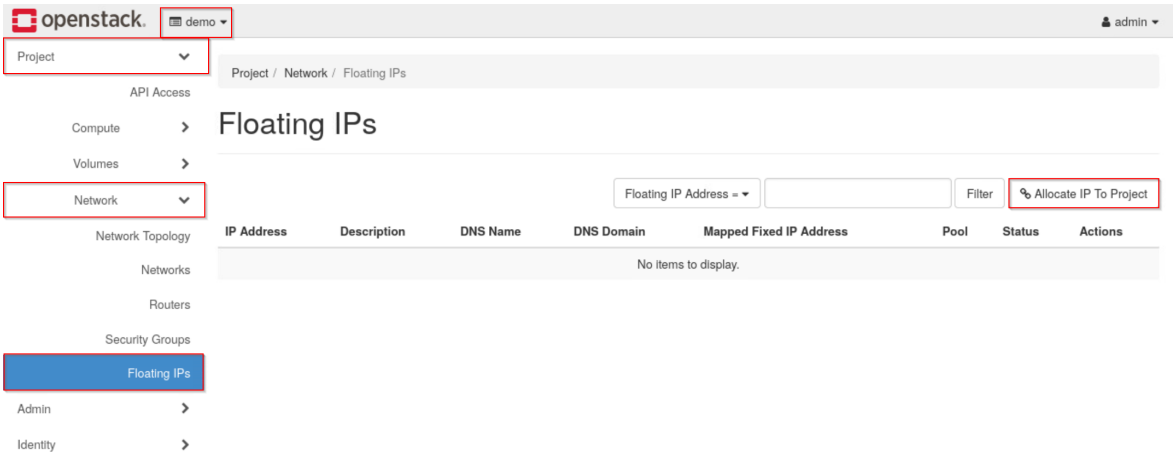
3.2. Create a new instance named **instance1**. Use the **ubuntu** image, **m1.small** flavor, and **shared** network.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --nic net-id=shared \
> instance1
```

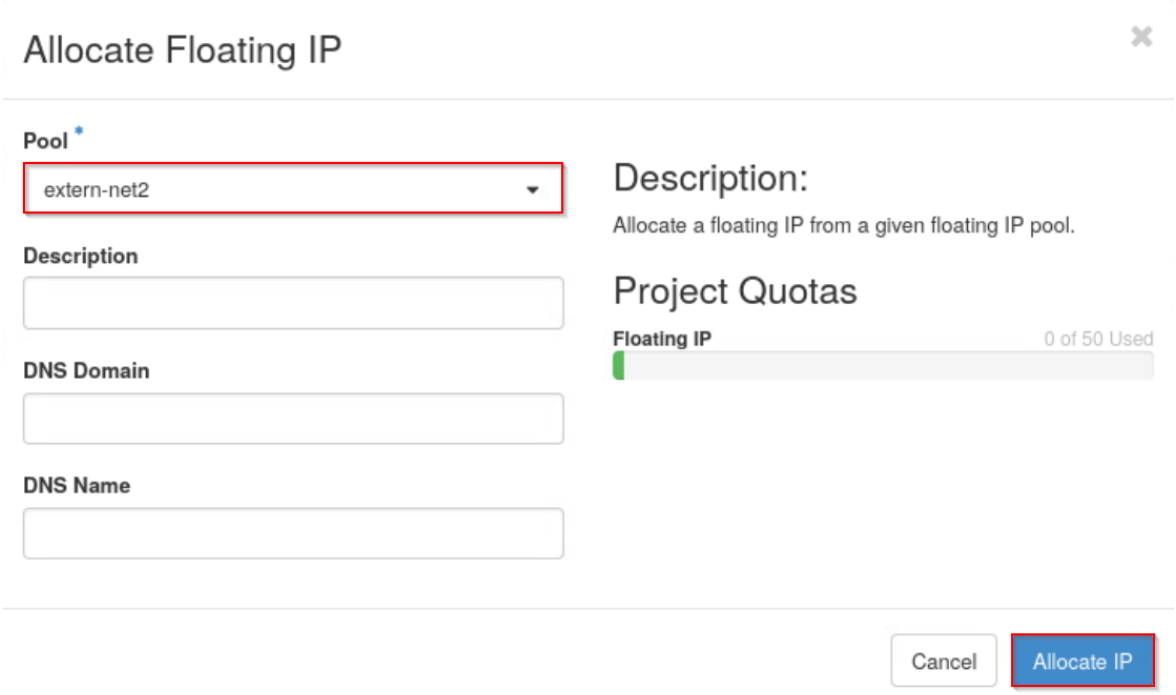
```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --nic net-id=shared \
> instance1
+-------------------------------------+------------------------------------------------+
| Field                               | Value                                          |
+-------------------------------------+------------------------------------------------+
| OS-DCF:diskConfig                   | MANUAL                                         |
| OS-EXT-AZ:availability_zone         |                                                |
| OS-EXT-SRV-ATTR:host                | None                                           |
| OS-EXT-SRV-ATTR:hypervisor_hostname | None                                           |
| OS-EXT-SRV-ATTR:instance_name       |                                                |
| OS-EXT-STS:power_state              | NOSTATE                                        |
| OS-EXT-STS:task_state               | scheduling                                     |
| OS-EXT-STS:vm_state                 | building                                       |
| OS-SRV-USG:launched_at              | None                                           |
| OS-SRV-USG:terminated_at            | None                                           |
| accessIPv4                          |                                                |
| accessIPv6                          |                                                |
| addresses                           |                                                |
| adminPass                           | wnVeGACMWPs7                                   |
| config_drive                        |                                                |
| created                             | 2024-06-17T21:36:11Z                           |
| flavor                              | m1.small (2)                                   |
| hostId                              |                                                |
| id                                  | 65fd940b-fe45-4acc-80e9-f282c4615fb0           |
| image                               | ubuntu (329d361e-f6dc-4b72-b200-3de0ec230e65)  |
| key_name                            | None                                           |
| name                                | instance1                                      |
| progress                            | 0                                              |
| project_id                          | 39e851b14f864573aad60582c35e40dc               |
| properties                          |                                                |
| security_groups                     | name='default'                                 |
| status                              | BUILD                                          |
| updated                             | 2024-06-17T21:36:10Z                           |
| user_id                             | 14f5376f00c04e90b7103dd8d4263040               |
| volumes_attached                    |                                                |
+-------------------------------------+------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

3.3. Leave the terminal window open and open the web browser. Navigate to **192.168.1.20**. Log into the *Horizon Dashboard* as the **admin** user with the password **secret**.

3.4. Switch to the **demo** project. Navigate to **Project** > **Network** > **Floating IPs**. Click **Allocate IP to Project**.



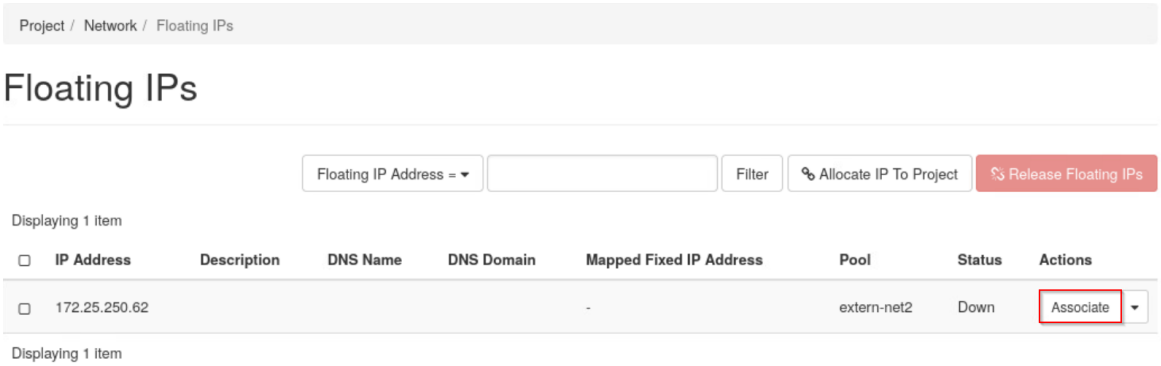
3.5. Ensure **extern-net2** is set as the *Pool*. Click **Allocate IP**.



Tip

A floating IP address can be deleted, or released, in multiple ways. One way is to select the checkbox next to the floating IP address, and click **Release Floating IPs**. Another way is to open the dropdown next to the **Associate** button in the same row as the floating IP address, then click **Release Floating IP**.

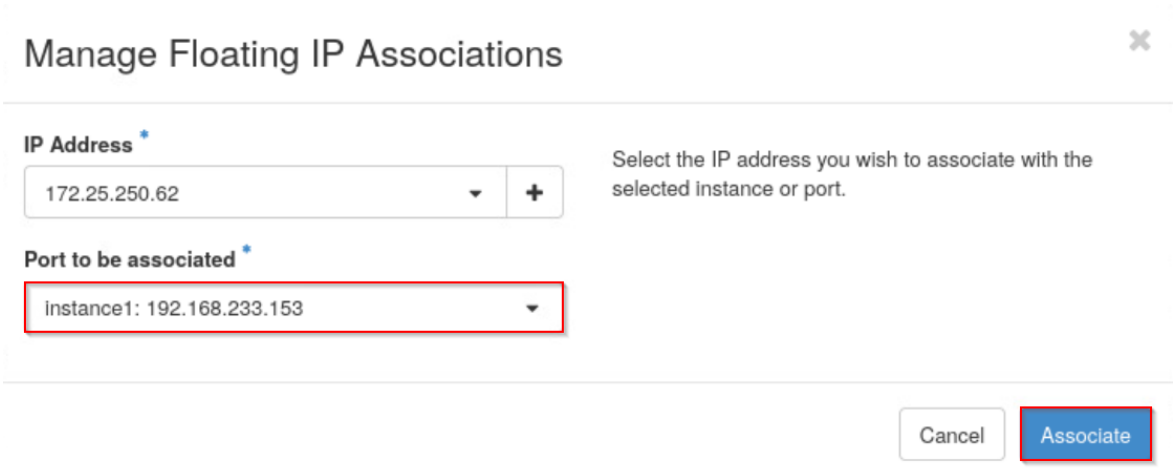
3.6. Click **Associate** in the row of the floating IP address.



Note

The actual value of the floating IP address may differ.

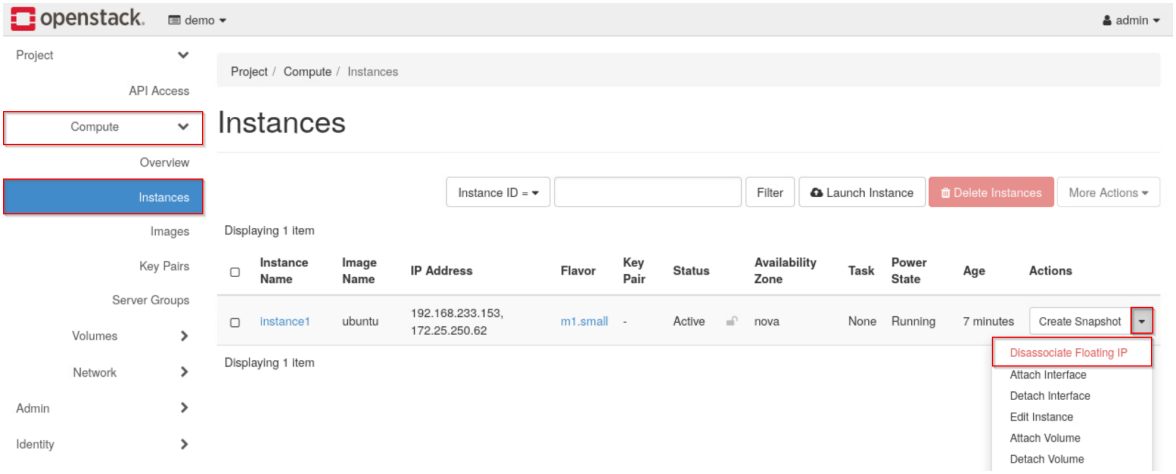
3.7. In the *Port to be associated* dropdown, select **instance1: 192.168.233.XYZ**. Click **Associate**.



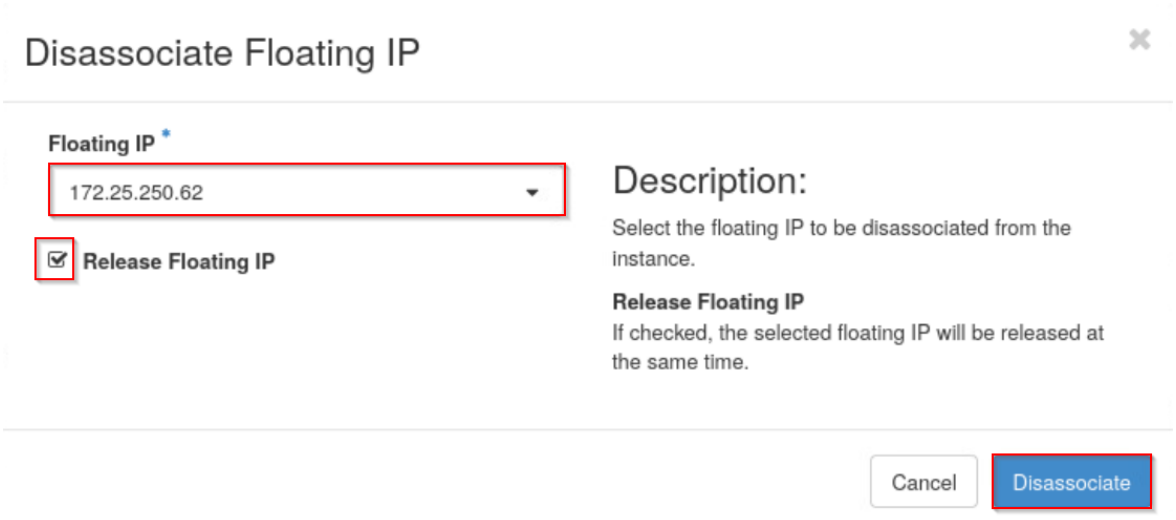
Note

The actual value of the instance's IP address may differ.

3.8. The **instance1** instance is now connected to the **extern-net2** network through this floating IP address. To remove a floating IP address, first navigate to **Compute** > **Instances**. Click the arrow next to the **Create Snapshot** in the same as **instance1**. Select **Disassociate Floating IP** to detach the floating IP from the instance.



3.9. Check the *Release Floating IP* box and click **Disassociate**.



Tip

A floating IP address can also be disassociated from the **Project** > **Network** > **Floating IPs** page. When a floating IP address has been associated with an instance, the button in the row of the floating IP address that used to read **Associate** will turn red and read **Disassociate**. Clicking this button will disassociate the floating IP address from its instance.

3.10. Log out of the *Horizon Dashboard* and close the web browser.

3.11. From the terminal, allocate a floating IP address in the **extern-net2** network.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip create \
> extern-net2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip create \
> extern-net2
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| created_at          | 2024-06-17T21:56:16Z                 |
| description         |                                      |
| fixed_ip_address    | None                                 |
| floating_ip_address | 172.25.250.75                        |
| floating_network_id | d1e72c9b-87be-4b48-aa49-a39b1f232e14 |
| id                  | 829baa74-65a3-4e33-9eb6-9785e7781bc5 |
| name                | 172.25.250.75                        |
| port_id             | None                                 |
| project_id          | 39e851b14f864573aad60582c35e40dc     |
| qos_policy_id       | None                                 |
| revision_number     | 0                                    |
| router_id           | None                                 |
| status              | DOWN                                 |
| subnet_id           | None                                 |
| updated_at          | 2024-06-17T21:56:16Z                 |
+---------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

You can use the **–floating-ip-address IP_ADDRESS** argument to allocate a specific IP address. However, make sure to list the available addresses before attempting to allocate it. If that particular floating IP address already exists, the command will throw an *HttpException: Conflict* error.

Tip

A floating IP address can be disassociated from and instance with the command **openstack floating ip remove INSTANCE FLOATING_IP_ADDRESS** and deleted with the command **openstack floating ip delete IP_ADDRESS**.

3.12. Associate the floating IP with **instance1**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server add \
> floating ip instance1 172.25.250.75
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server add floating ip \
> instance1 172.25.250.75
[ubuntu@workstation (keystone-admin)]:~$
```

> **Note**
>
> The actual floating IP may differ. Use the floating IP address generated from your output from the previous step.

3.13. We will recreate this instance at the end of the lab once the rest of the necessary resources have been created. We will not need this instance anymore, so delete it. This will also disassociate the floating IP address, but it will still be available.

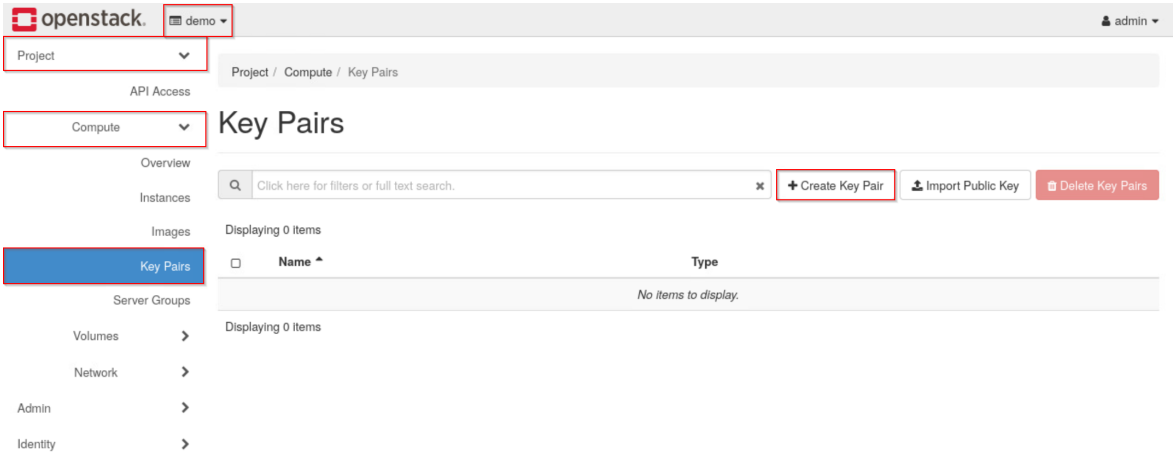
```
[ubuntu@workstation (keystone-admin)]:~$ openstack server delete instance1
```

3.14. Leave the terminal window open and continue to the next task.

4 Managing SSH Key Pairs

In this task, you will use the *Horizon Dashboard* and *OpenStack Unified CLI* to manage SSH key pairs that will be used later in the lab to connect to OpenStack instances from outside the OpenStack environment.

4.1. Switch to the **demo** project and navigate to **Project** > **Compute** > **Key Pairs**. Click **Create Key Pair** to create a new key pair.



4.2. Enter **keypair1** in the *Key Pair Name* field, and select **SSH Key** in the *Key Type* dropdown. Click **Create Key Pair**. This will create the key pair and download it to the **~/Downloads** directory.

Tip

Key pairs can be deleted from the Horizon Dashboard the same way as other objects. Simply select the checkbox next to the key pair you wish to delete, then click **Delete Key Pairs**.

4.3. Sign out of the Horizon Dashboard and close the web browser.

4.4. If a terminal window is not already open, open one and source the **admin** credentials from the **~/keystonerc-admin** file.

```
ubuntu@workstation:~$ source ~/keystonerc-admin
```

```
ubuntu@workstation:~$ source ~/keystonerc-admin
[ubuntu@workstation (keystone-admin)]:~$
```

4.5. We only need one key pair to connect to the external instance, so the key pair created from the Horizon Dashboard can safely be deleted in order to demonstrate creating a key pair from the command line. Delete the **keypair1** key pair.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack keypair delete keypair1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack keypair delete keypair1
[ubuntu@workstation (keystone-admin)]:~$
```

Note

Note that a key pair in the context of OpenStack is actually a misnomer. The key pair object really only refers to the public key, while the private key only exists in the file in which it is saved. Therefore, the private key file will still exist after deleting the key pair.

4.6. Delete the private key located at **~/Downloads/keypair1.pem**.

```
[ubuntu@workstation (keystone-admin)]:~$ rm -f ~/Downloads/keypair1.pem
```

```
[ubuntu@workstation (keystone-admin)]:~$ rm -f ~/Downloads/keypair1.pem
[ubuntu@workstation (keystone-admin)]:~$
```

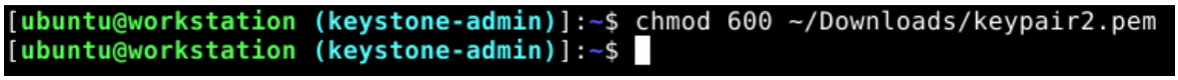
4.7. Create the key pair **keypair2** and save the private key to the file **~/Downloads/keypair2.pem**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack keypair create \
> keypair2 > ~/Downloads/keypair2.pem
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack keypair create \
> keypair2 > ~/Downloads/keypair2.pem
[ubuntu@workstation (keystone-admin)]:~$
```

4.8. To better protect the private key, use the **chmod** command with a mode of **600** to make it so that the **ubuntu** user has read/write permissions on the private key file, and groups and other users have no permissions to the file.

```
[ubuntu@workstation (keystone-admin)]:~$ chmod 600 ~/Downloads/keypair2.pem
```



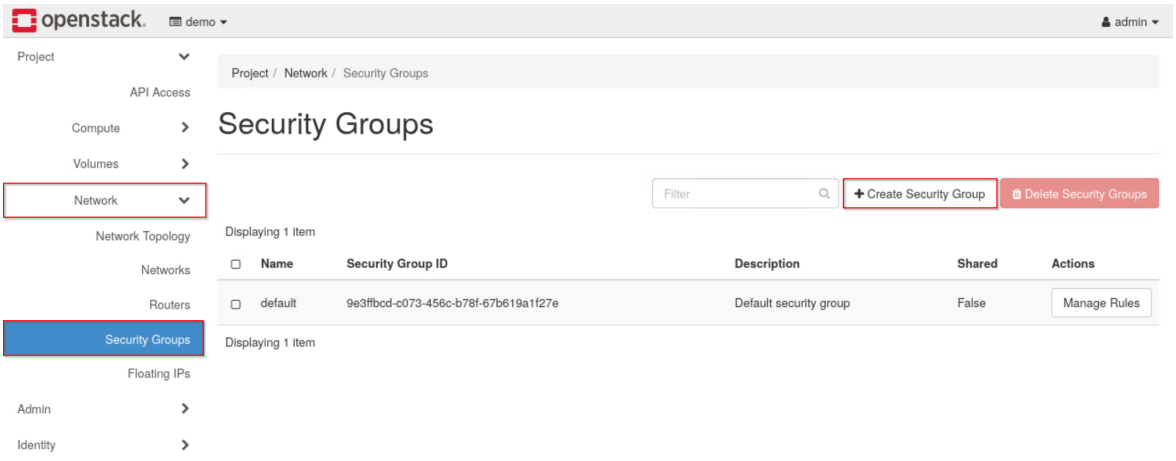
4.9. Leave the terminal window open and continue to the next task.

5 Implementing Security

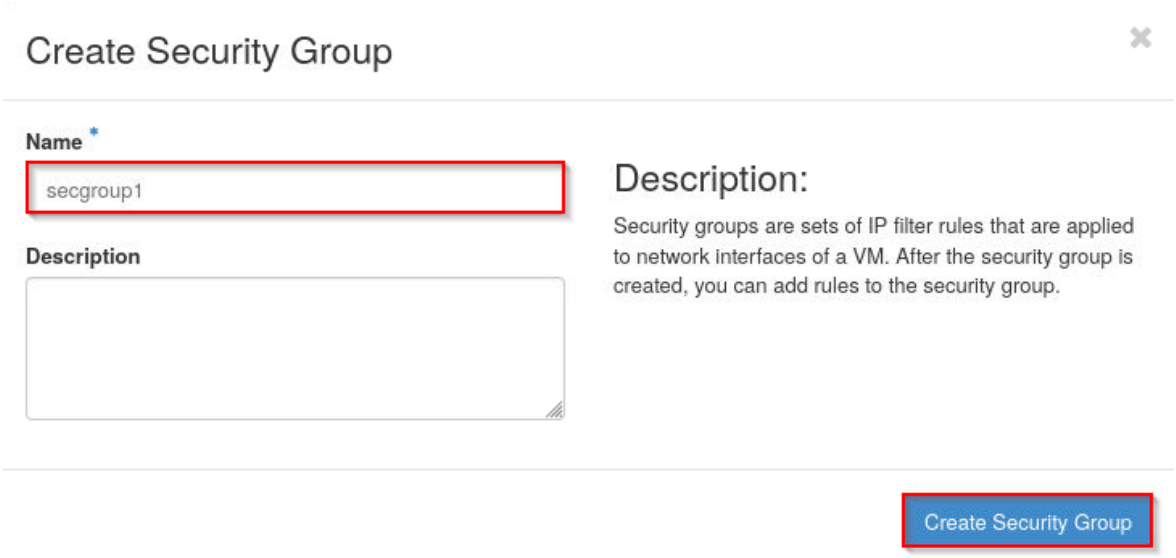
In this task, you will use the *Horizon Dashboard* and *OpenStack Unified CLI* to manage security groups for OpenStack instances. This is similar to constructing firewall rules and will be used to allow certain types of network traffic while disallowing others.

5.1. Open the web browser and navigate to **192.168.1.20**. Log into the dashboard as **admin** with the password **secret**.

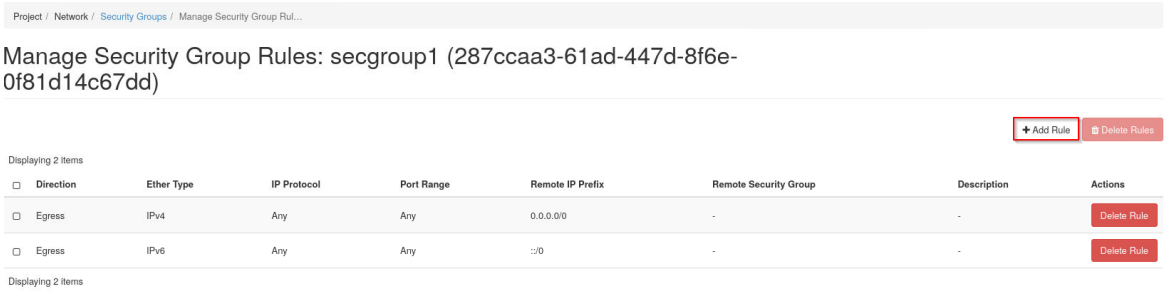
5.2. Switch to the **demo** project. Navigate to **Network** > **Security Groups** and click **Create Security Group**.



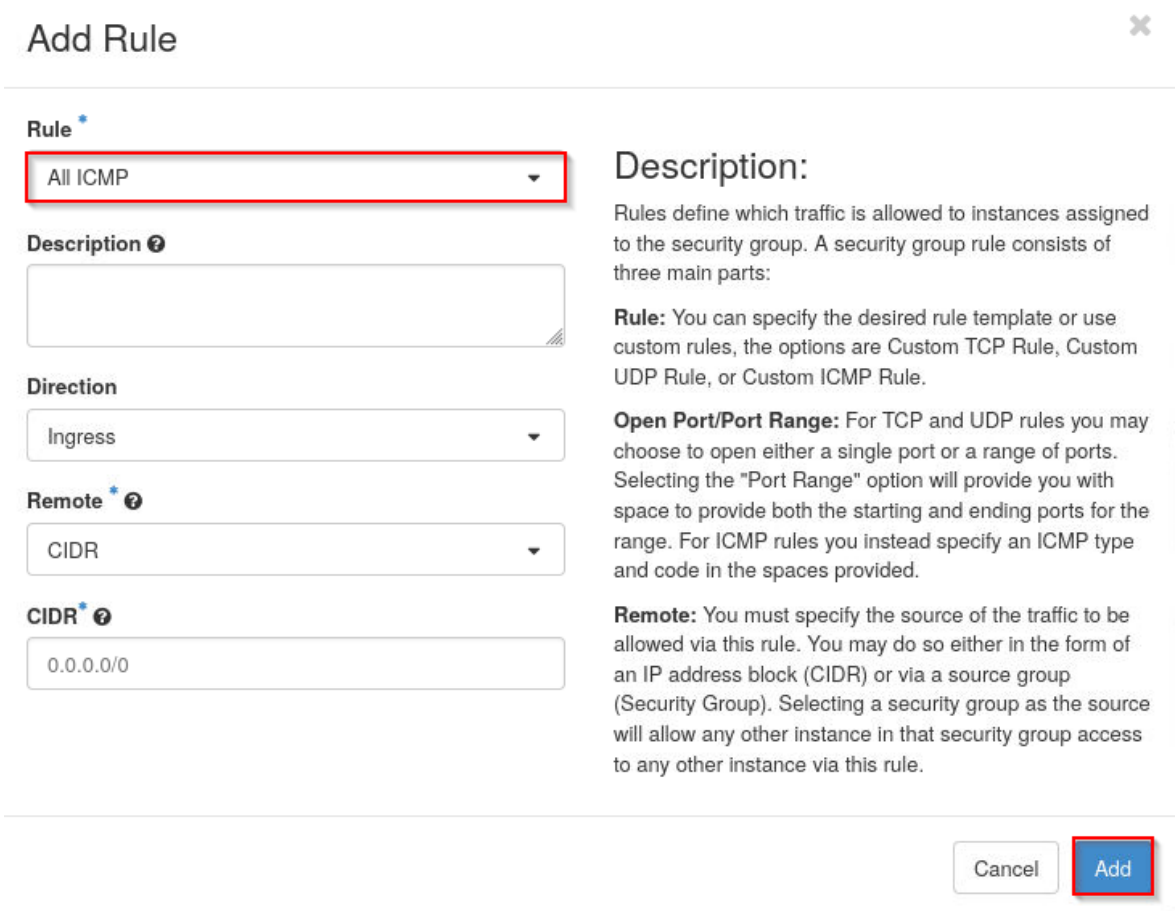
5.3. Enter **secgroup1** into the *Name* field and click **Create Security Group**.



5.4. After creating the security group, you should land on the page containing the rules for the security group. If not, click **Manage Rules** in the same column as **secgroup1** on the **Security Groups** page to get there. From here, you can see that by default, the security group allows any egress (outgoing) traffic and does not allow any ingress (incoming) traffic. Click **Add Rule** to add a new rule in the security group.



5.5. Select **All ICMP** from the *Rule* dropdown and click **Add**. This allows ICMP traffic, namely the **ping** command, to reach instances in this security group.



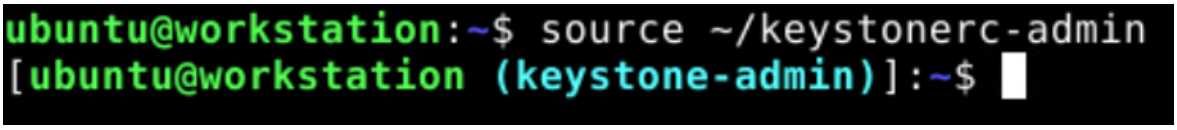
Note

By default, *Direction* is set to **Ingress** and *CIDR* is set to **0.0.0.0/0**. **Ingress** specifies incoming traffic, and **0.0.0.0/0** specifies that the traffic is accepted from any IP address.

5.6. Log out of the *Horizon Dashboard* and close the web browser.

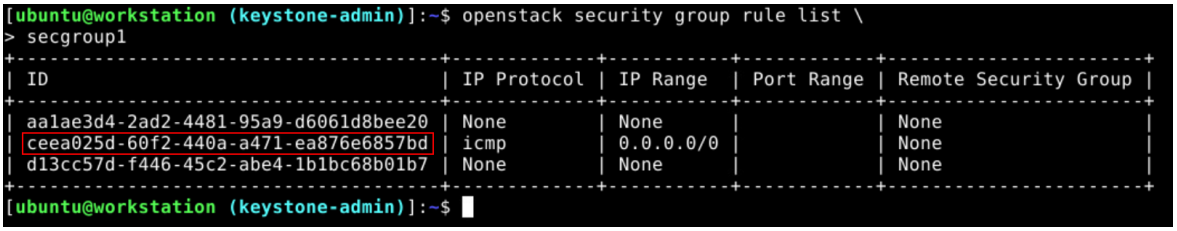
5.7. If a terminal window is not already open, open one and source the **admin** credentials from the **~/keystonerc-admin** file.

```
ubuntu@workstation:~$ source ~/keystonerc-admin
```



5.8. Next, we will recreate this security group through the command line and add some additional rules necessary for connecting to an external instance. First, to demonstrate how to remove a rule from a security group, list the rules in the **secgroup1** security group and copy the ID of the ICMP rule.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup1
```

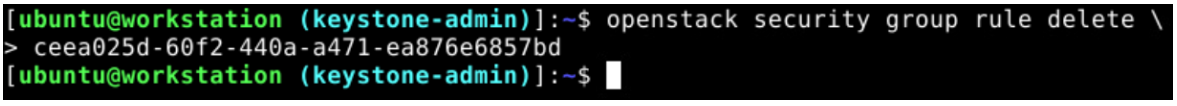


Tip

To copy a value from the terminal, select the desired string with the mouse, then either right-click and click **Copy** or press **Ctrl+Shift+C**.

5.9. Use the *ID* for the ICMP rule to delete that rule.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule delete \
> ceeea025d-60f2-440a-a471-ea876e6857bd
```



Note

The actual ID value may differ.

Tip

To paste a value to the command line, either right-click and click **Paste** or press **Ctrl+Shift+V**.

5.10. List the rules in the **secgroup1** security group again to ensure the rule was deleted successfully.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup1
```

5.11. Delete the **secgroup1** security group.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group delete \
> secgroup1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group delete \
> secgroup1
[ubuntu@workstation (keystone-admin)]:~$
```

5.12. Create the **secgroup2** security group.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group create \
> --max-width 80 secgroup2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group create \
> --max-width 80 secgroup2
+-----------------+-----------------------------------------------------------+
| Field           | Value                                                     |
+-----------------+-----------------------------------------------------------+
| created_at      | 2024-06-18T00:37:29Z                                      |
| description     | secgroup2                                                 |
| id              | 2b65be6a-5951-4e92-b6ab-ff4e92872131                      |
| name            | secgroup2                                                 |
| project_id      | 39e851b14f864573aad60582c35e40dc                          |
| revision_number | 1                                                         |
| rules           | created_at='2024-06-18T00:37:29Z', direction='egress',    |
|                 | ethertype='IPv4', id='26d3fced-                           |
|                 | 5be0-4e57-9cc9-dd0d151dbfe1', standard_attr_id='76',      |
|                 | updated_at='2024-06-18T00:37:29Z'                         |
|                 | created_at='2024-06-18T00:37:29Z', direction='egress',    |
|                 | ethertype='IPv6', id='326b3e26-9430-4acd-                 |
|                 | aba9-8010060e91c3', standard_attr_id='75',                |
|                 | updated_at='2024-06-18T00:37:29Z'                         |
| updated_at      | 2024-06-18T00:37:29Z                                      |
+-----------------+-----------------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

5.13. List the rules in the **secgroup2** security group. These are the default rules that exist upon creation.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup2
+--------------------------------------+-------------+----------+------------+-----------------------+
| ID                                   | IP Protocol | IP Range | Port Range | Remote Security Group |
+--------------------------------------+-------------+----------+------------+-----------------------+
| 26d3fced-5be0-4e57-9cc9-dd0d151dbfe1 | None        | None     |            | None                  |
| 326b3e26-9430-4acd-aba9-8010060e91c3 | None        | None     |            | None                  |
+--------------------------------------+-------------+----------+------------+-----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

You can use the command **openstack security group rule show RULE_ID** to show the details of each rule and confirm that they are the same default rules you get when creating a security group through the Horizon Dashboard. The rules allow all outgoing traffic over IPv4 and IPv6.

5.14. Add a security rule in the **secgroup2** security group to allow all incoming ICMP traffic.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule create \
> --protocol icmp \
> secgroup2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule create \
> --protocol icmp \
> secgroup2
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| created_at        | 2024-06-18T00:46:15Z                 |
| description       |                                      |
| direction         | ingress                              |
| ether_type        | IPv4                                 |
| id                | 94eb94e8-ae83-4c9f-8d00-acd0b1217dd6 |
| name              | None                                 |
| port_range_max    | None                                 |
| port_range_min    | None                                 |
| project_id        | 39e851b14f864573aad60582c35e40dc     |
| protocol          | icmp                                 |
| remote_group_id   | None                                 |
| remote_ip_prefix  | 0.0.0.0/0                            |
| revision_number   | 0                                    |
| security_group_id | 2b65be6a-5951-4e92-b6ab-ff4e92872131 |
| updated_at        | 2024-06-18T00:46:15Z                 |
+-------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

> **Note**
>
> If no arguments are given, the direction defaults to **ingress** and the remote IP defaults to **0.0.0.0/0**. In other words, it allows all incoming traffic over the given protocol.

5.15. List the rules in the **secgroup2** security group again to ensure the ICMP rule was created successfully.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup2
```

5.16. Add another security rule to allow remote connection using SSH on the default port 22.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule create \
> --protocol tcp \
> --dst-port 22 \
> secgroup2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule create \
> --protocol tcp \
> --dst-port 22 \
> secgroup2
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| created_at        | 2024-06-18T00:48:35Z                 |
| description       |                                      |
| direction         | ingress                              |
| ether_type        | IPv4                                 |
| id                | b1722675-bf7f-4a05-89cc-e76bfa1c009c |
| name              | None                                 |
| port_range_max    | 22                                   |
| port_range_min    | 22                                   |
| project_id        | 39e851b14f864573aad60582c35e40dc     |
| protocol          | tcp                                  |
| remote_group_id   | None                                 |
| remote_ip_prefix  | 0.0.0.0/0                            |
| revision_number   | 0                                    |
| security_group_id | 2b65be6a-5951-4e92-b6ab-ff4e92872131 |
| updated_at        | 2024-06-18T00:48:35Z                 |
+-------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

5.17. List the rules in the **secgroup2** security group again to ensure the SSH rule was created successfully.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup2
```

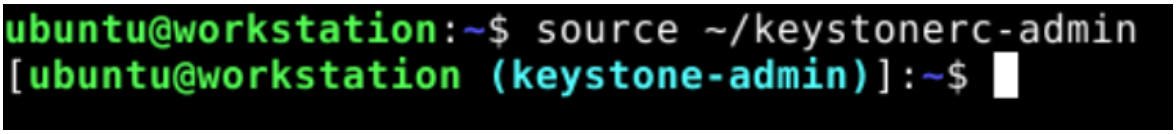
5.18. Leave the terminal window open and continue to the next task.

6 Launching and Verifying an External Instance

Up to this point, we have created an external network, a router, a floating IP address, an SSH key pair, and a security group. These are all the resources necessary to create and interact with an external instance from outside the OpenStack cloud. In this task, you will launch an external instance and verify its connectivity and functionality with the **ssh** and **ping** commands.

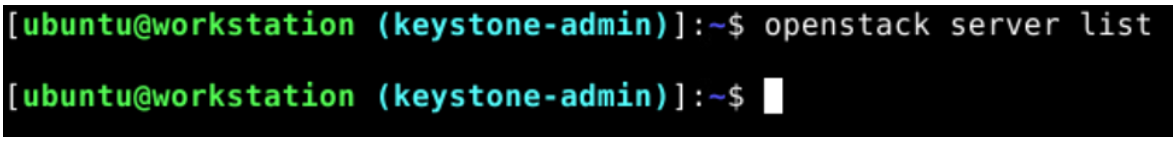
6.1. If a terminal window is not already open, open one and source the admin credentials from the ~**/keystonerc-admin** file.

```
ubuntu@workstation:~$ source ~/keystonerc-admin
```



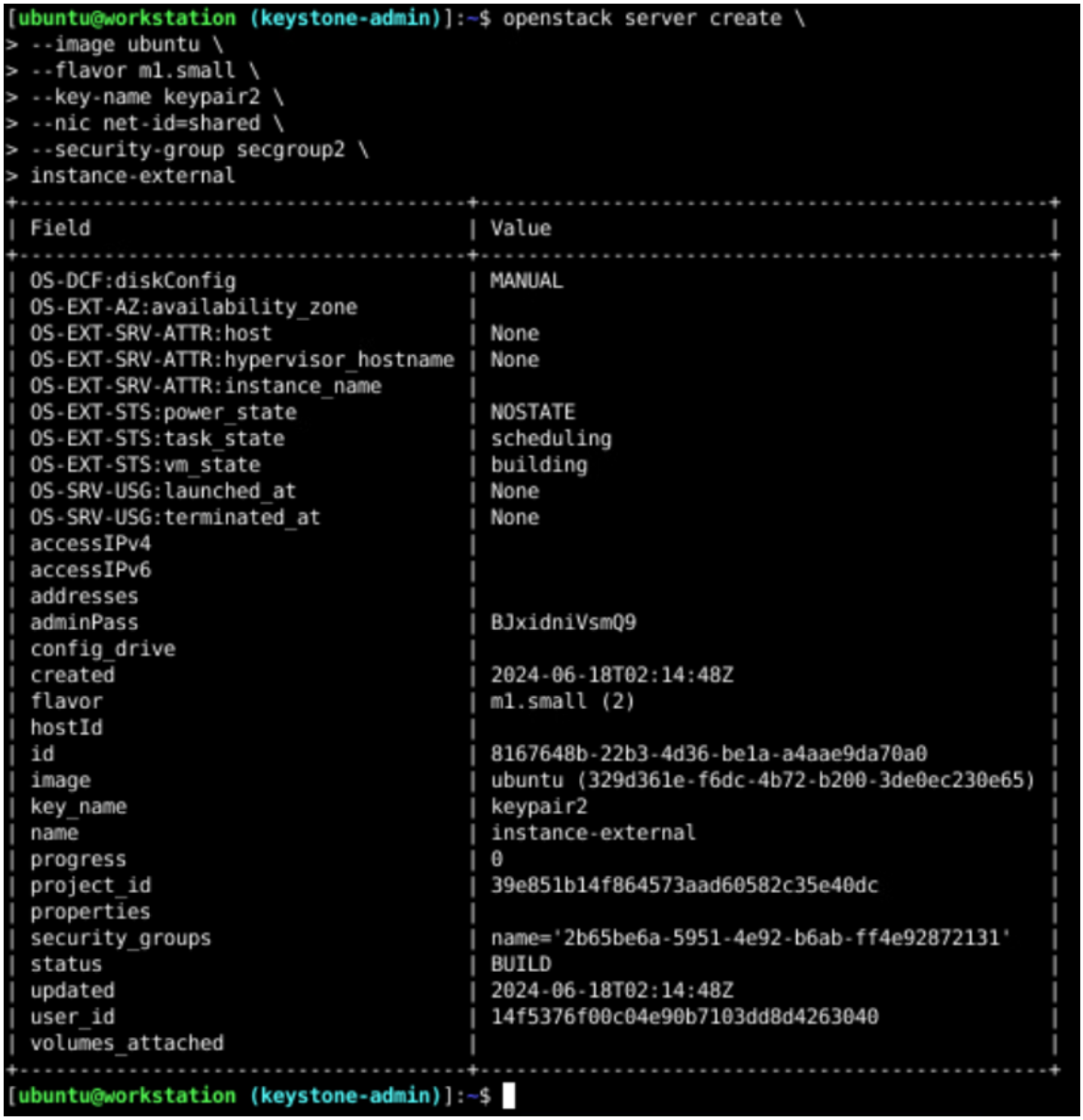
6.2. List all instances in the project. The list should be empty.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server list
```



6.3. Launch an instance named **instance-external** with the **ubuntu** image, the **m1.small** flavor, the **keypair2** key pair, the **shared** network, and the **secgroup2** security group.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --key-name keypair2 \
> --nic net-id=shared \
> --security-group secgroup2 \
> instance-external
```



6.4. List the floating IPs.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip list \
> --max-width 90
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip list \
> --max-width 90
+--------------+--------------------+-----------------+------+-----------------+----------------+
| ID           | Floating IP Address | Fixed IP Address | Port | Floating Network | Project        |
+--------------+--------------------+-----------------+------+-----------------+----------------+
| 829baa74-65a3 | 172.25.250.75      | None            | None | d1e72c9b-87be-4b | 39e851b14f86457 |
| -4e33-9eb6-97 |                    |                 |      | 48-aa49-a39b1f23 | 3aad60582c35e40 |
| 85e7781bc5    |                    |                 |      | 2e14             | dc              |
+--------------+--------------------+-----------------+------+-----------------+----------------+
[ubuntu@workstation (keystone-admin)]:~$
```

6.5. Associate the floating IP address with the **instance-external** instance.

```
ubuntu@workstation;~$ openstack server add floating ip \
> instance-external 172.25.250.75
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server add floating ip \
> instance-external 172.25.250.75
[ubuntu@workstation (keystone-admin)]:~$
```

Note

Be sure to use the floating IP address that matches your output as they may differ slightly from this example.

6.6. Verify that the instance was assigned the floating IP address.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server list \
> -c Name \
> -c Networks
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server list \
> -c Name \
> -c Networks
+-------------------+----------------------------------------+
| Name              | Networks                               |
+-------------------+----------------------------------------+
| instance-external | shared=192.168.233.164, 172.25.250.75 |
+-------------------+----------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

For commands that output tables, you can pull out only the columns you want with the **-c** option followed by the column name. This option can be chained as in the command above to list multiple columns.

6.7. Use the **scp** command to send the **keypair2** key pair to the **devstack** machine over SSH. Use the password **ubuntu** for authentication.

```
[ubuntu@workstation (keystone-admin)]:~$ scp ~/Downloads/keypair2.pem \
> ubuntu@192.168.1.20:~/keypair2.pem
```

```
[ubuntu@workstation (keystone-admin)]:~$ scp ~/Downloads/keypair2.pem \
> ubuntu@192.168.1.20:~/keypair2.pem
ubuntu@192.168.1.20's password:
keypair2.pem                                  100% 1680     2.2MB/s   00:00
[ubuntu@workstation (keystone-admin)]:~$
```

6.8. SSH into the **devstack** machine. Use the password **ubuntu** when prompted.

```
[ubuntu@workstation (keystone-admin)]:~$ ssh 192.168.1.20
```

```
[ubuntu@workstation (keystone-admin)]:~$ ssh 192.168.1.20
ubuntu@192.168.1.20's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Mon Jun 17 21:23:08 2024 from 192.168.1.21
ubuntu@devstack:~$
```

6.9. Ping the **instance-external** instance with the floating IP that was assigned to it in the previous task.

```
ubuntu@devstack:~$ ping -c3 172.25.250.75
```

```
ubuntu@devstack:~$ ping -c3 172.25.250.75
PING 172.25.250.75 (172.25.250.75) 56(84) bytes of data.
64 bytes from 172.25.250.75: icmp_seq=1 ttl=63 time=22.4 ms
64 bytes from 172.25.250.75: icmp_seq=2 ttl=63 time=2.28 ms
64 bytes from 172.25.250.75: icmp_seq=3 ttl=63 time=1.44 ms

--- 172.25.250.75 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.441/8.700/22.383/9.681 ms
ubuntu@devstack:~$
```

Note

You should receive three successful ping replies.

6.10. SSH into the **instance-external** instance with the **keypair2.pem** file. Enter **yes** when asked if you want to continue.

```
ubuntu@devstack:~$ ssh -i ~/keypair2.pem \
> 172.25.250.75
```

```
ubuntu@devstack:~$ ssh -i ~/keypair2.pem \
> 172.25.250.75
The authenticity of host '172.25.250.75 (172.25.250.75)' can't be established.
ED25519 key fingerprint is SHA256:fC1zXRxeRHheK1oLk/2sgvaMEKXkXw4UzTCh8W5Txhs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.25.250.75' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-92-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Tue Jun 18 02:28:02 UTC 2024

  System load:  0.2001953125      Processes:             84
  Usage of /:   7.4% of 19.20GB   Users logged in:       0
  Memory usage: 8%                IPv4 address for ens3: 192.168.233.164
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@instance-external:~$
```

Note

It may take a few minutes for the instance to be fully booted and ready to accept SSH connections.

> **Note**
>
> It is important to connect to the instance through SSH from the **devstack** machine since it is outside the OpenStack cloud. A successful connection verifies the external connectivity of the instance.

6.11. Ping the DHCP server on the **shared** network to verify connectivity.

```
ubuntu@instance-external:~$ ping -c3 192.168.233.2
```

```
ubuntu@instance-external:~$ ping -c3 192.168.233.2
PING 192.168.233.2 (192.168.233.2) 56(84) bytes of data.
64 bytes from 192.168.233.2: icmp_seq=1 ttl=64 time=5.15 ms
64 bytes from 192.168.233.2: icmp_seq=2 ttl=64 time=2.67 ms
64 bytes from 192.168.233.2: icmp_seq=3 ttl=64 time=0.729 ms

--- 192.168.233.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.729/2.852/5.154/1.810 ms
ubuntu@instance-external:~$
```

> **Note**
>
> You should receive three successful ping replies.

6.12. The lab is now complete.