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 security groups.
- Create and manage SSH key pairs.
- Launch and verify an external instance.

Lab Settings

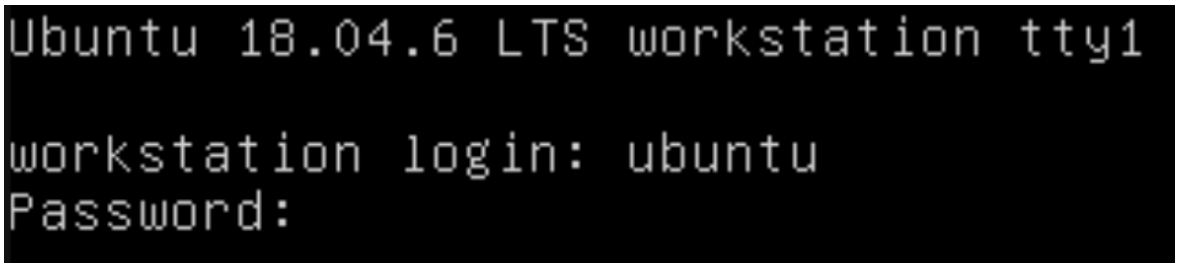
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

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

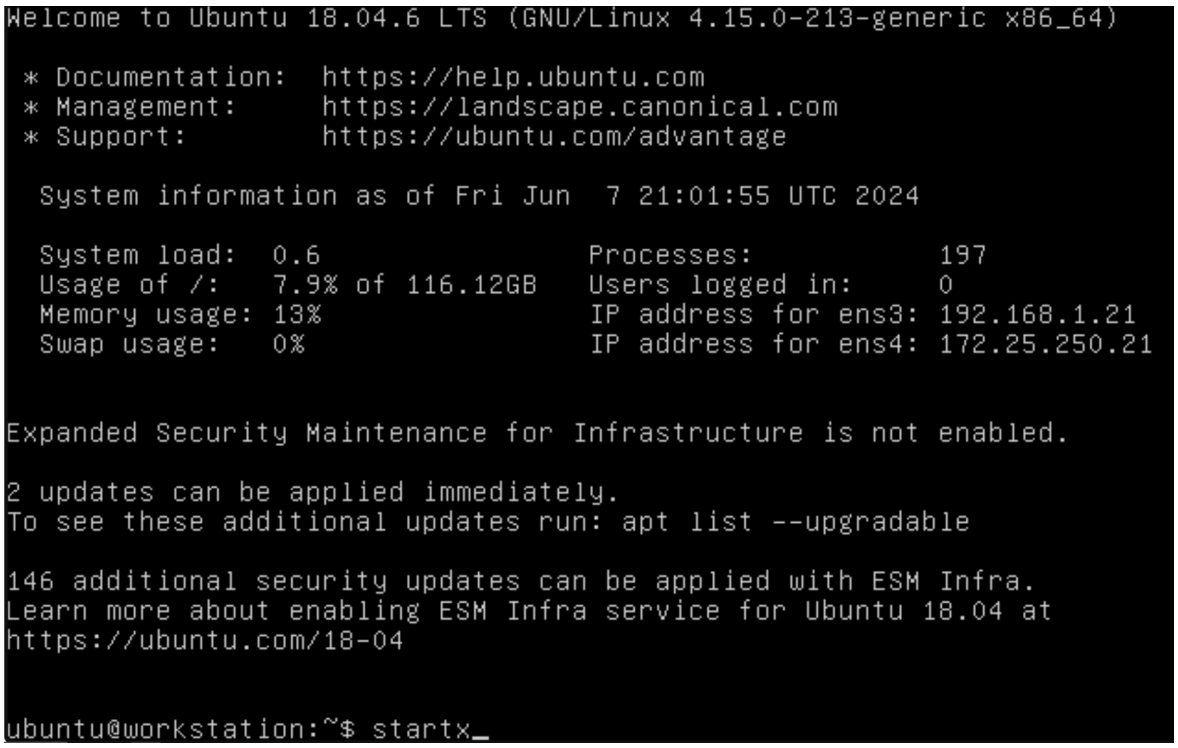
In this task, you will use the *Horizon Dashboard* and the **OpenStack Unified CLI** to create and configure an external network. Resources on this network will be accessible to users outside the OpenStack environment.

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



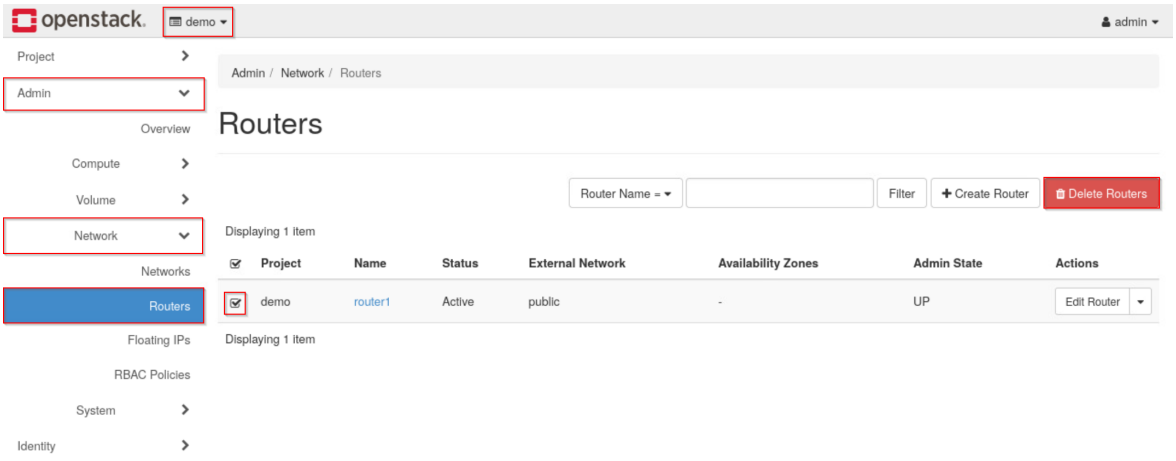
1.2. Launch the graphical user interface.

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

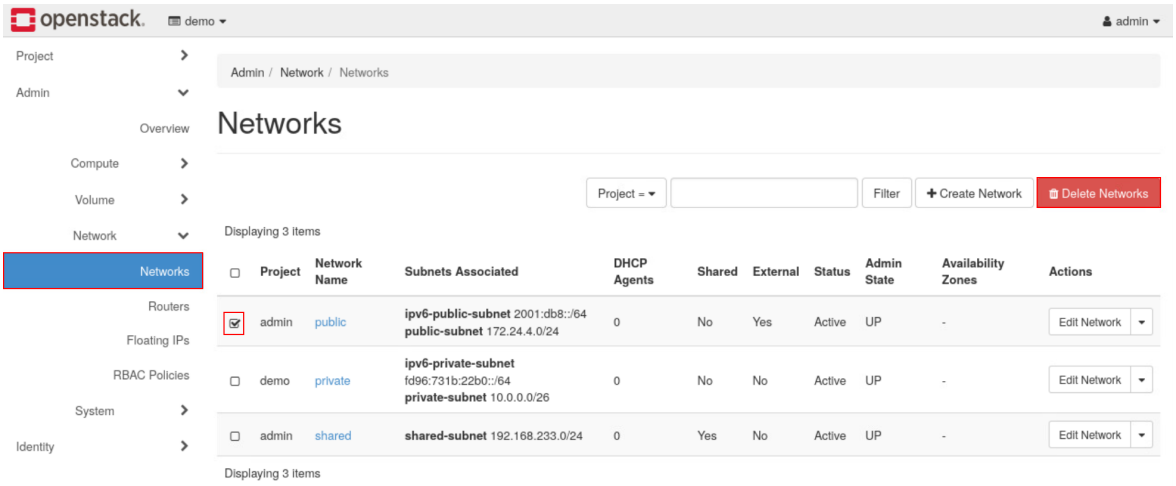


1.3. Open the web browser. Navigate to **192.168.1.20** and log in to the dashboard as **admin** with the password **secret**. In this lab, we will create our own public network and router. The **demo** project already has a default router and public network, so those need to be deleted first.

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



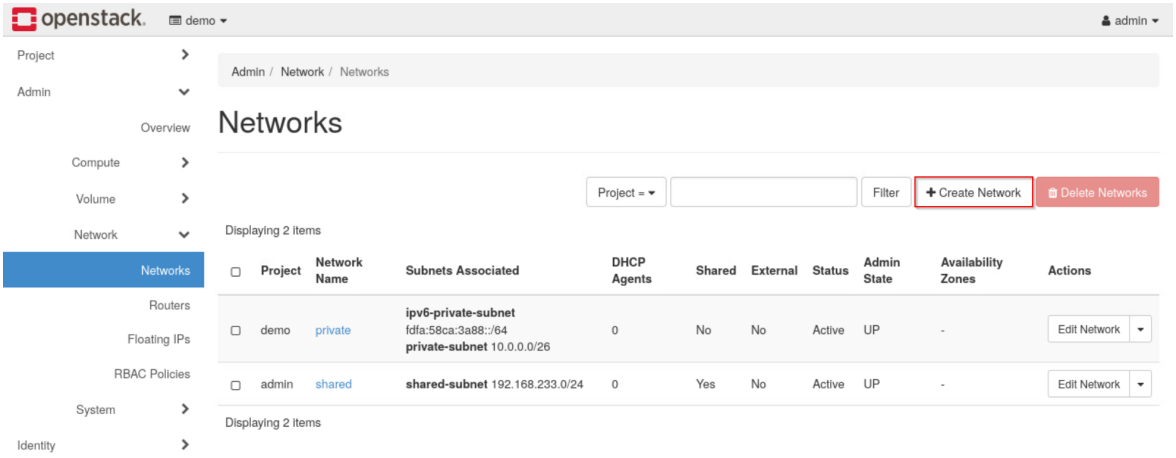
1.5. Now, navigate to **Networks**. Check the box in the same row as **public**, then click **Delete Networks**.



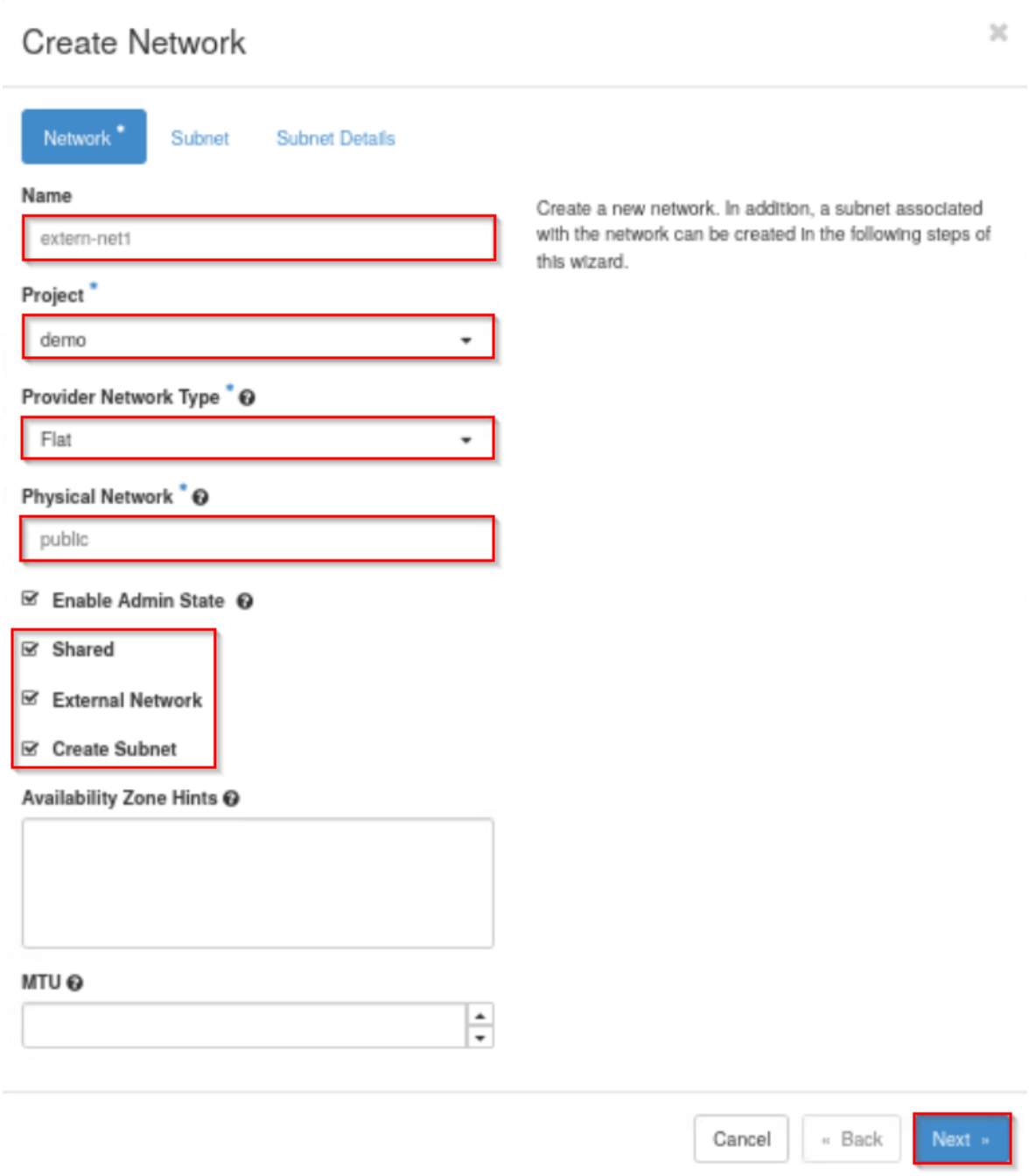
Note

If you try to delete the **public** network before deleting the router, you will receive an error saying "one or more ports still exist on the requested network". Therefore, it is necessary to delete any external interfaces (gateways) that exist on routers attached to a network before deleting the network. When a router is deleted, all of its ports are automatically deleted.

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.



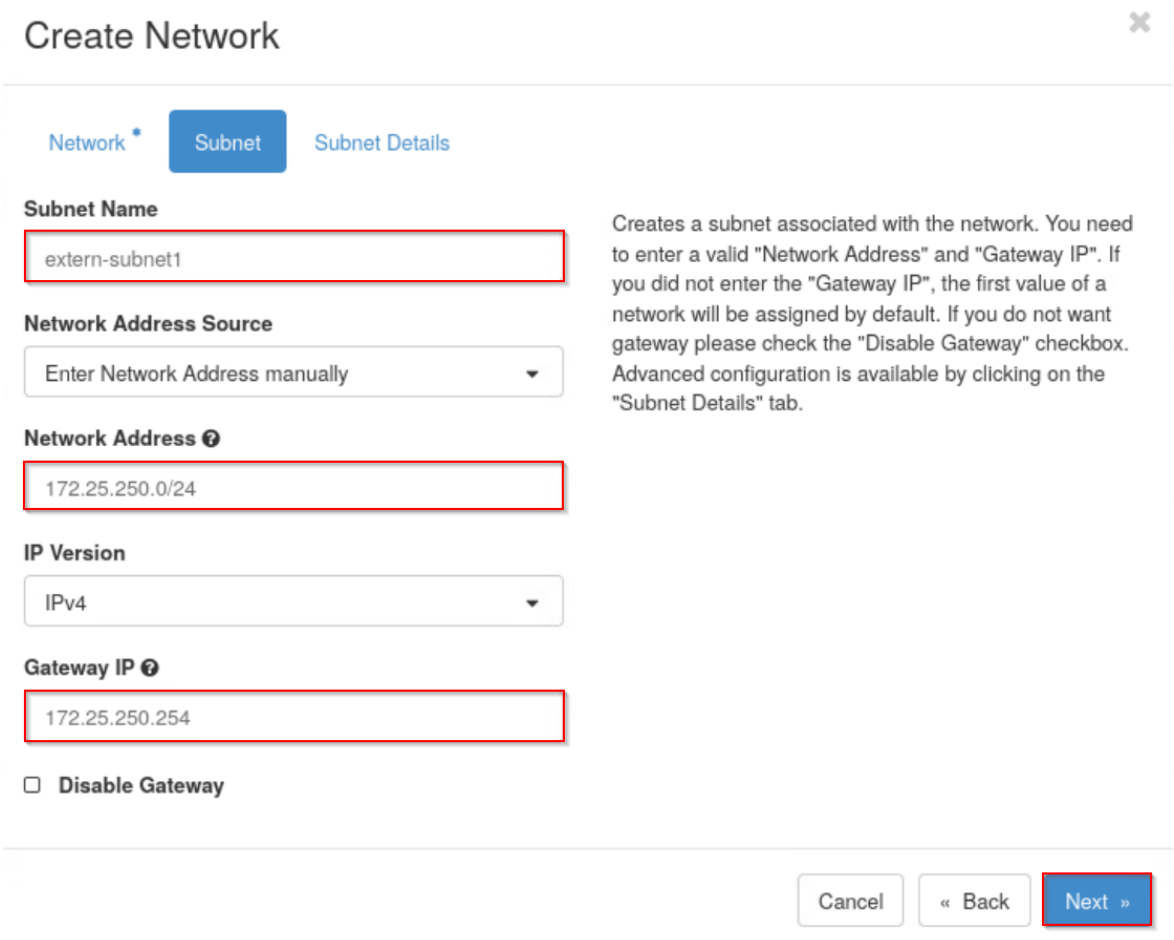
Note

The **public** physical network you will use in this task is not the same as the **public** network you just deleted. The deleted network was a virtual network built on top of a physical network, and they just happen to have the same name. The physical **public** network still exists because it is a separate resource used by OpenStack for external communication.

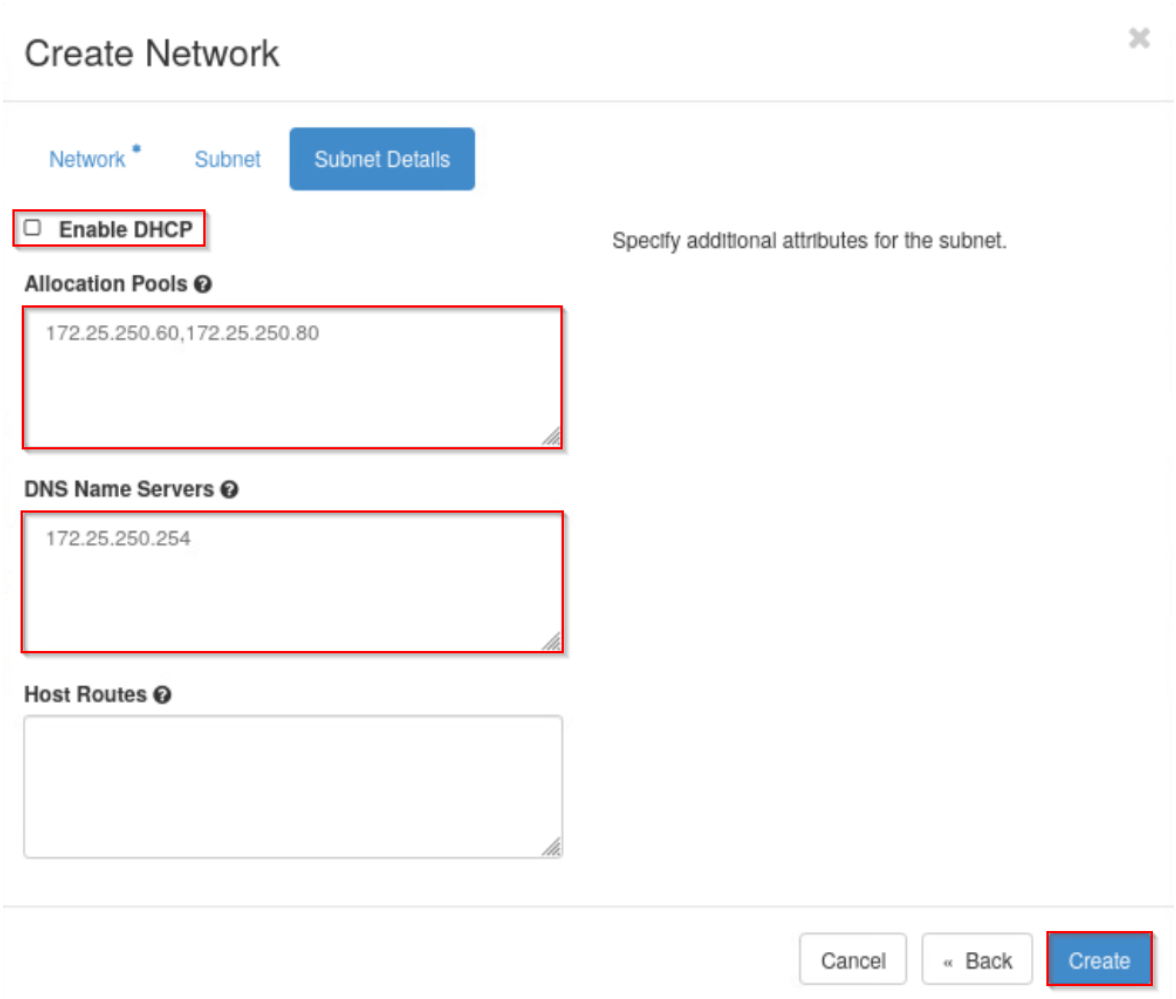
Tip

If your **Create Network** form looks different, you likely navigated to **Project** > **Network** > **Networks**. You can only create external networks from the **Admin** > **Network** > **Networks** tab.

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
```

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

1.12. List the available networks.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list
+--------------------------------------+-------------+--------------------------------------+
| ID                                   | Name        | Subnets                              |
+--------------------------------------+-------------+--------------------------------------+
| 966ecb4f-                            | private     | 674205b6-1357-4727-a21a-             |
| 4ff8-44ea-a476-2d2f18955085          |             | 94220492a57f, fa8a2545-5a8c-         |
|                                      |             | 44a2-bacc-1b86c253b880               |
| 9f23266f-d833-4337-9a27-4818a        | shared      | 7e456257-76e5-4cfc-bf3f-             |
| 6d28e9e                              |             | b2a3876dba40                         |
| fbe1af81-a185-43c6-be35-93c17        | extern-net1 | 3a53569e-7246-4c3f-b051-dc51b9       |
| 8ed7720                              |             | efbaa8                               |
+--------------------------------------+-------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

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
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list
+--------------------------------------+---------+--------------------------------------+
| ID                                   | Name    | Subnets                              |
+--------------------------------------+---------+--------------------------------------+
| 966ecb4f-                            | private | 674205b6-1357-4727-a21a-             |
| 4ff8-44ea-a476-2d2f18955085          |         | 94220492a57f, fa8a2545-5a8c-44a2     |
|                                      |         | -bacc-1b86c253b880                   |
| 9f23266f-d833-4337-9a27-4818a6d      | shared  | 7e456257-76e5-4cfc-bf3f-             |
| 28e9e                                |         | 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                | 2025-06-28T14:10:30Z                 |
| description               |                                      |
| dns_domain                | None                                 |
| id                        | acdc9bc2-56a3-466e-8d27-141c8f71ae99 |
| 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                | 2025-06-28T14:10:30Z                 |
+---------------------------+--------------------------------------+
[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        | 2025-06-28T14:12:56Z                 |
| description       |                                      |
| dns_nameservers   | 172.25.250.254                       |
| enable_dhcp       | False                                |
| gateway_ip        | 172.25.250.254                       |
| host_routes       |                                      |
| id                | e320bd2f-d0d2-46ba-832a-286ed3e2841c |
| ip_version        | 4                                    |
| ipv6_address_mode | None                                 |
| ipv6_ra_mode      | None                                 |
| name              | extern-subnet2                       |
| network_id        | acdc9bc2-56a3-466e-8d27-141c8f71ae99 |
| project_id        | 39e851b14f864573aad60582c35e40dc     |
| revision_number   | 0                                    |
| segment_id        | None                                 |
| service_types     |                                      |
| subnetpool_id     | None                                 |
| tags              |                                      |
| updated_at        | 2025-06-28T14:12:56Z                 |
+-------------------+--------------------------------------+
[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
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list
+--------------------------------------+-------------+--------------------------------------+
| ID                                   | Name        | Subnets                              |
+--------------------------------------+-------------+--------------------------------------+
| 966ecb4f-                            | private     | 674205b6-1357-4727-a21a-             |
| 4ff8-44ea-a476-2d2f18955085          |             | 94220492a57f, fa8a2545-5a8c-         |
|                                      |             | 44a2-bacc-1b86c253b880               |
| 9f23266f-d833-4337-9a27-4818a        | shared      | 7e456257-76e5-4cfc-bf3f-             |
| 6d28e9e                              |             | b2a3876dba40                         |
| acdc9bc2-56a3-466e-                  | extern-net2 | e320bd2f-d0d2-46ba-832a-             |
| 8d27-141c8f71ae99                    |             | 286ed3e2841c                         |
+--------------------------------------+-------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

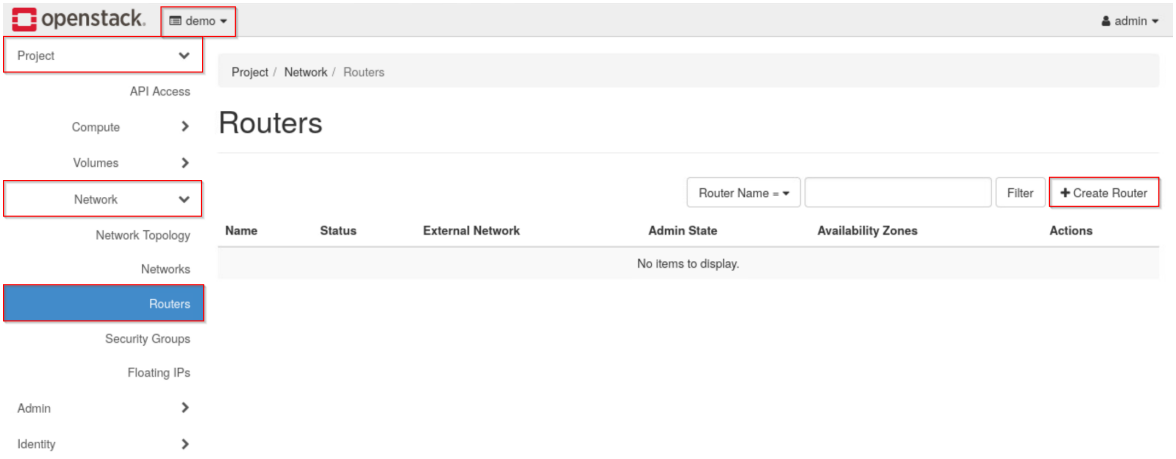
1.18. Leave the terminal window open and continue to the next task.

2 Preparing OpenStack Routers to Deploy an Instance

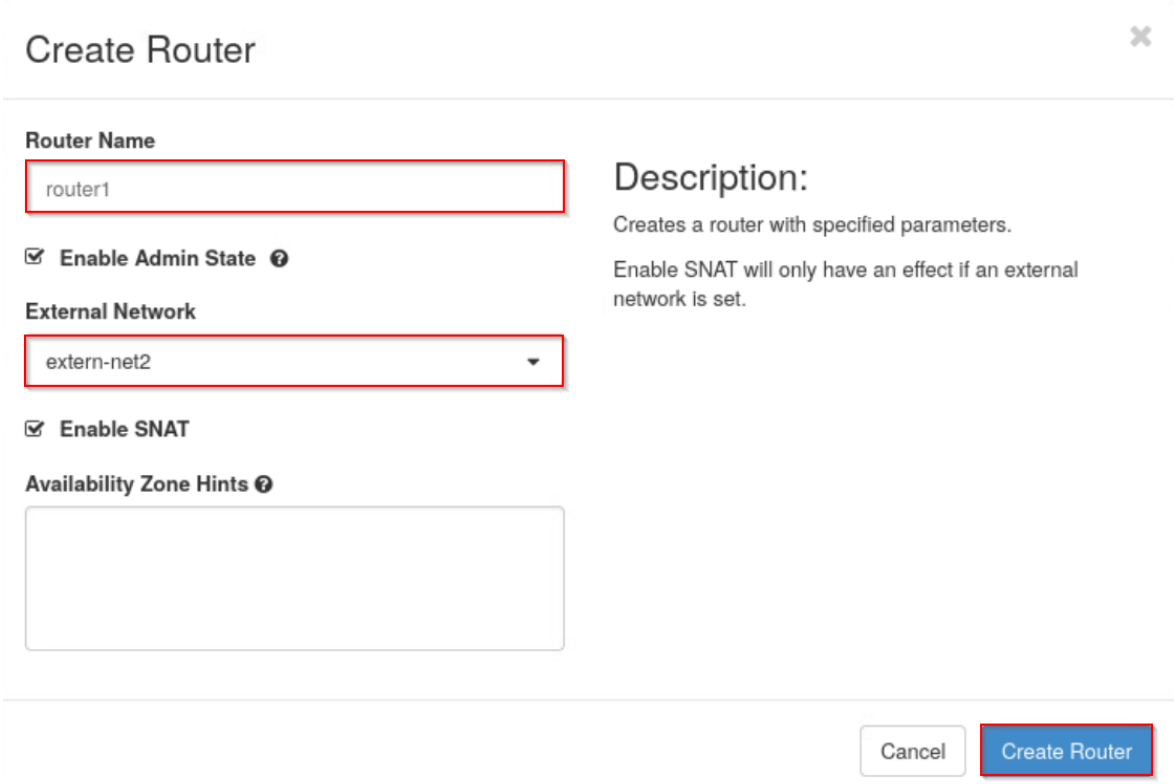
In this task, you will create and configure a router with the *Horizon Dashboard* and *OpenStack CLI* and use command line tools to test the connectivity of the router. The router will serve to connect resources on the external network to other networks both within OpenStack and outside the cloud.

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

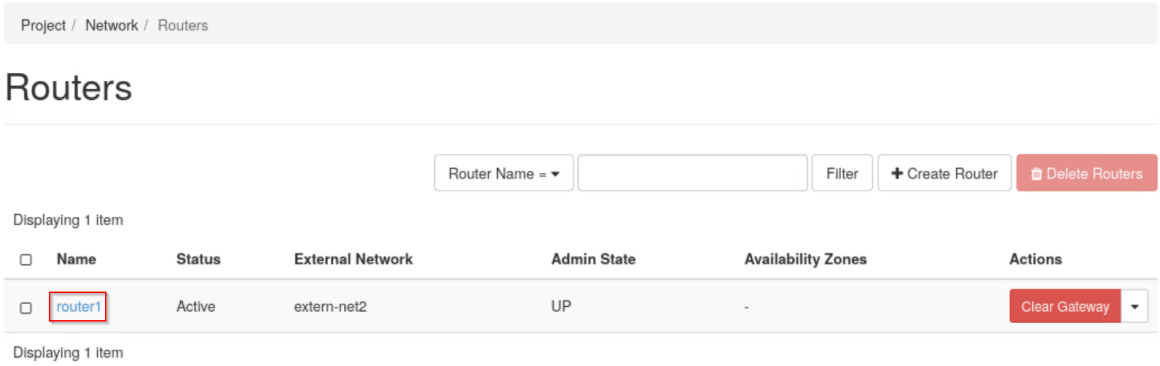
2.2. Select the **demo** project and navigate to **Project** > **Network** > **Routers**. Click **Create Router** to create a new router.



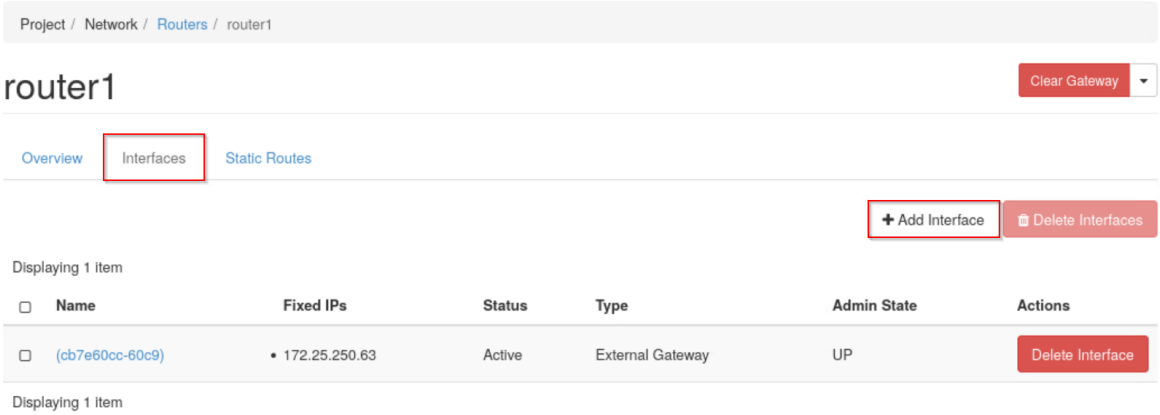
2.3. Enter **router1** in the *Router Name* field and select **extern-net2** in the *External Network* dropdown. Click **Create Router**.



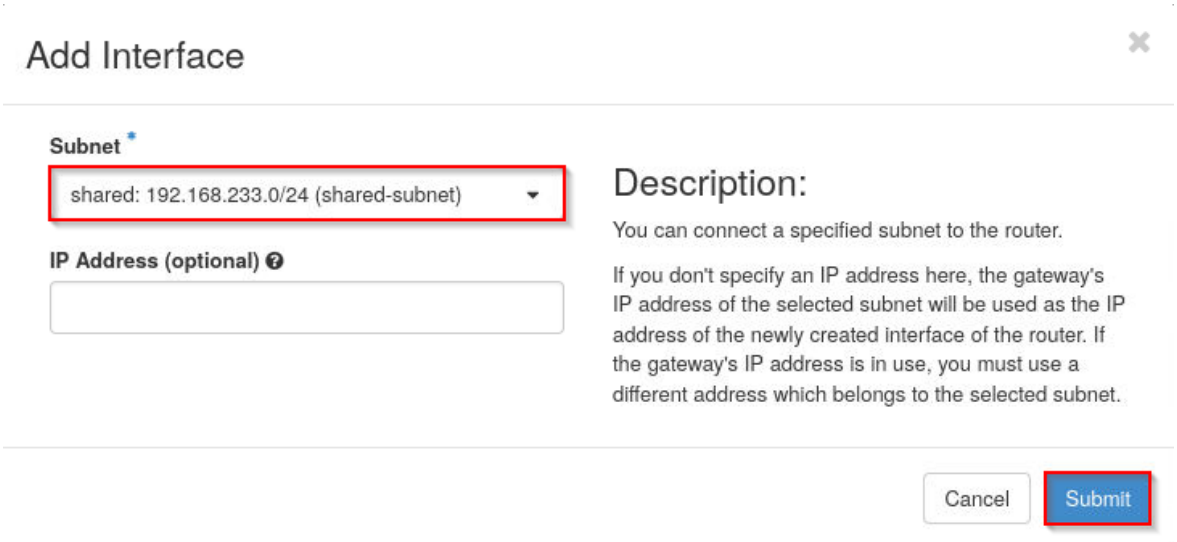
2.4. Click the router name, **router1**, to access its details.



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 need to delete **router1**. In the Horizon Dashboard, this process is straightforward: deleting a router automatically removes its interfaces. However, when using the CLI, the process requires a few extra steps. Try deleting **router1**; you should receive an error.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router delete router1
Failed to delete router with name or ID 'router1': Unable to delete Router for o
penstack.network.v2.router.Router(status=ACTIVE, external_gateway_info={u'networ
k_id': u'b138cfcc-c305-44b4-bf54-0f5926d5e14d', u'enable_snat': True, u'external
_fixed_ips': [{u'subnet_id': u'bdf0b17f-bd27-43a9-81eb-e7050bcb522c', u'ip_addre
ss': u'172.25.250.77'}]}, availability_zone_hints=[], availability_zones=[], nam
e=router1, admin_state_up=True, tenant_id=39e851b14f864573aad60582c35e40dc, crea
ted_at=2025-07-03T15:50:51Z, tags=[], updated_at=2025-07-03T15:51:17Z, descripti
on=, routes=[], id=25781270-fb3b-48c0-8eaf-e14335e92a8d, revision=4)
1 of 1 routers failed to delete.
[ubuntu@workstation (keystone-admin)]:~$
```

2.10. This error occurs because the CLI does not allow a router to be deleted while it is still connected to networks. To proceed, we must first disconnect the routers by removing any attached subnets. In this case, we already know the name of the subnet: **shared-subnet** on the **shared** network. Later in the lab, you'll learn how to automate this process even when you don't know the names of the subnets. For now, remove the connection to **shared-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)]:~$
```

2.11. Unset the external gateway of 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)]:~$
```

Tip

Since we know that the external gateway goes through **extern-net2**, we could have also used this command:

```
openstack router remove subnet router1 extern-net2
```

2.12. Delete the **router1** router.

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

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

2.13. 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              | 2025-06-28T14:16:48Z                 |
| description             |                                      |
| distributed             | False                                |
| external_gateway_info   | None                                 |
| flavor_id               | None                                 |
| ha                      | False                                |
| id                      | 52cd25aa-b97a-41e0-9c78-0c50331abc43 |
| name                    | router2                              |
| project_id              | 39e851b14f864573aad60582c35e40dc     |
| revision_number         | 1                                    |
| routes                  |                                      |
| status                  | ACTIVE                               |
| tags                    |                                      |
| updated_at              | 2025-06-28T14:16:48Z                 |
+-------------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

2.14. 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)]:~$
```

2.15. 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)]:~$
```

2.16. 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 router2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router show router2
+-------------------------+-----------------------------------------------------+
| Field                   | Value                                               |
+-------------------------+-----------------------------------------------------+
| admin_state_up          | UP                                                  |
| availability_zone_hints |                                                     |
| availability_zones      |                                                     |
| created_at              | 2025-06-28T14:16:48Z                                |
| description             |                                                     |
| distributed             | False                                               |
| external_gateway_info   | {"network_id": "acdc9bc2-56a3-466e-                 |
|                         | 8d27-141c8f71ae99", "enable_snat": true,            |
|                         | "external_fixed_ips": [{"subnet_id": "e320bd2f-     |
|                         | d0d2-46ba-832a-286ed3e2841c", "ip_address":         |
|                         | "172.25.250.66"}]}                                  |
| flavor_id               | None                                                |
| ha                      | False                                               |
| id                      | 52cd25aa-b97a-41e0-9c78-0c50331abc43                |
| interfaces_info         | [{"subnet_id": "7e456257-76e5-4cfc-bf3f-            |
|                         | b2a3876dba40", "ip_address": "192.168.233.1",       |
|                         | "port_id": "a3382b05-e1ac-42af-858d-                |
|                         | f73ea0aca60c"}]                                     |
| name                    | router2                                             |
| project_id              | 39e851b14f864573aad60582c35e40dc                    |
| revision_number         | 4                                                   |
| routes                  |                                                     |
| status                  | ACTIVE                                              |
| tags                    |                                                     |
| updated_at              | 2025-06-28T14:18:04Z                                |
+-------------------------+-----------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

2.17. 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.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Sat Jun 28 14:20:04 2025 from 192.168.1.21
ubuntu@devstack:~$
```

2.18. 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 172.25.250.66
```

```
ubuntu@devstack:~$ ping -c3 172.25.250.66
PING 172.25.250.66 (172.25.250.66) 56(84) bytes of data.
64 bytes from 172.25.250.66: icmp_seq=1 ttl=254 time=26.4 ms
64 bytes from 172.25.250.66: icmp_seq=2 ttl=254 time=0.586 ms
64 bytes from 172.25.250.66: icmp_seq=3 ttl=254 time=0.550 ms

--- 172.25.250.66 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.550/9.173/26.383/12.169 ms
ubuntu@devstack:~$
```

Note

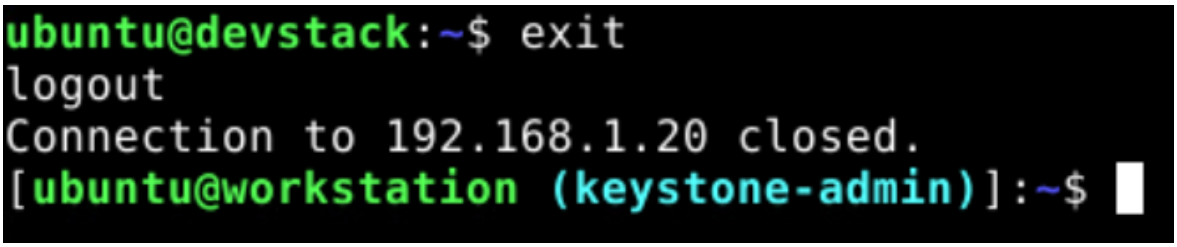
The actual IP address may differ from this example.

Note

You should receive three successful ping replies.

2.19. Exit the SSH session.

```
ubuntu@devstack:~$ exit
```



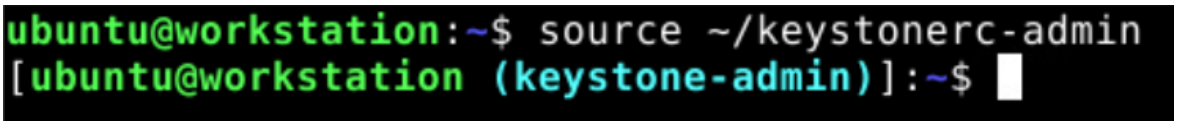
2.20. Leave the terminal window open and continue to the next task.

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
```



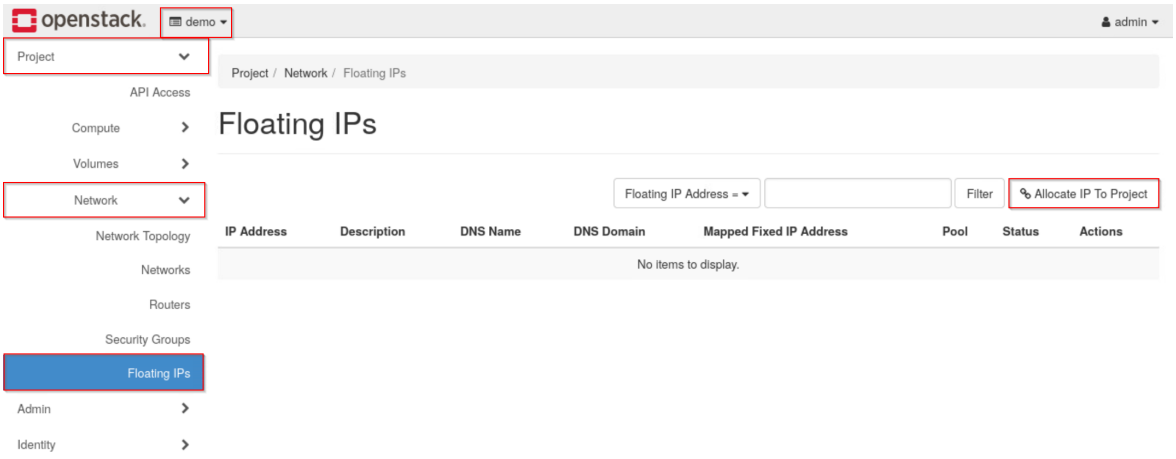
3.2. Create a new instance named **instance1**. Use the **ubuntu** image, **m1.small** flavor, and **shared** network.

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

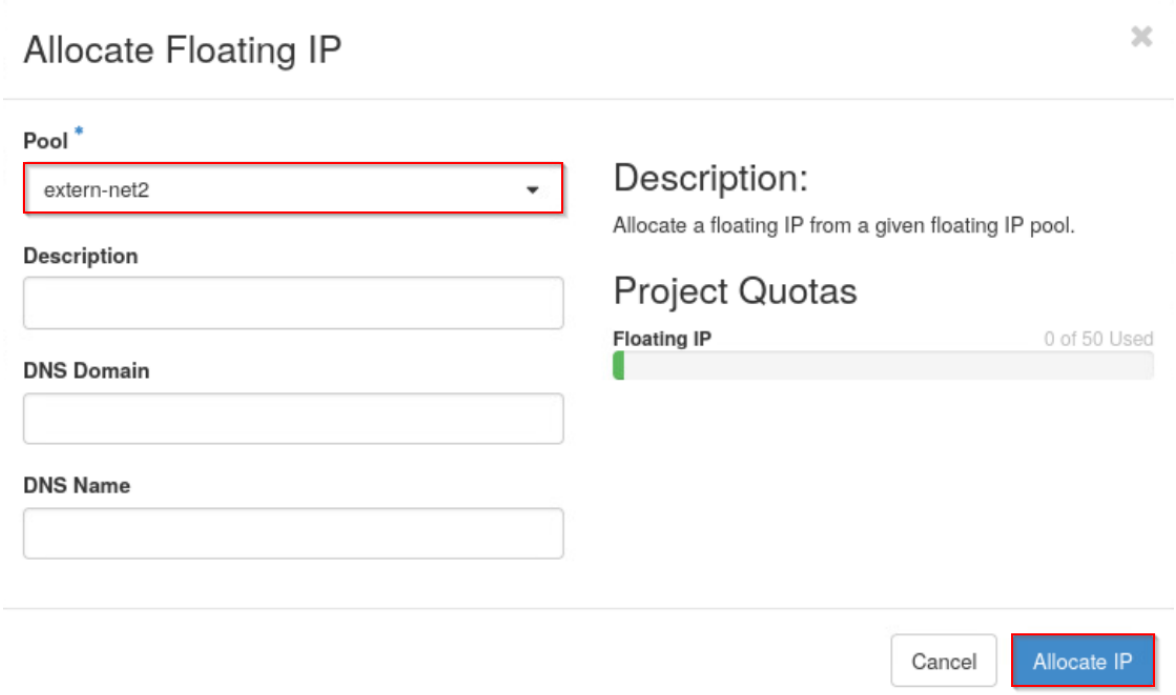
```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --network shared \
> instance1
+-------------------------------------+--------------------------------------+
| Field                               | Value                                |
+-------------------------------------+--------------------------------------+
| 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                           | 7BBQbMzMdkr6                         |
| config_drive                        |                                      |
| created                             | 2025-06-28T14:22:11Z                 |
| flavor                              | m1.small (2)                         |
| hostId                              |                                      |
| id                                  | 693c9a39-5469-44e9-a5c1-99061286dab0 |
| 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                             | 2025-06-28T14:22:11Z                 |
| 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. Select the **demo** project. Navigate to **Project** > **Network** > **Floating IPs**. Click **Allocate IP to Project**.



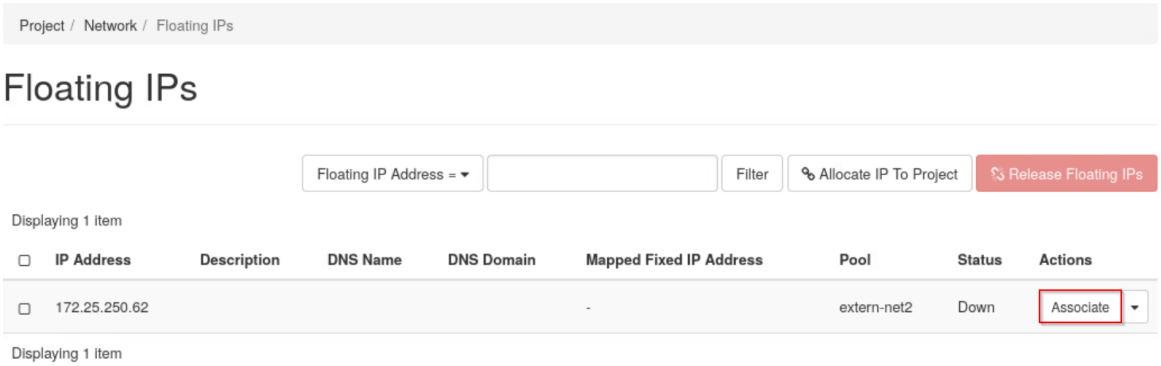
3.5. Ensure **extern-net2** is set as the *Pool*. Click **Allocate IP**.



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**.

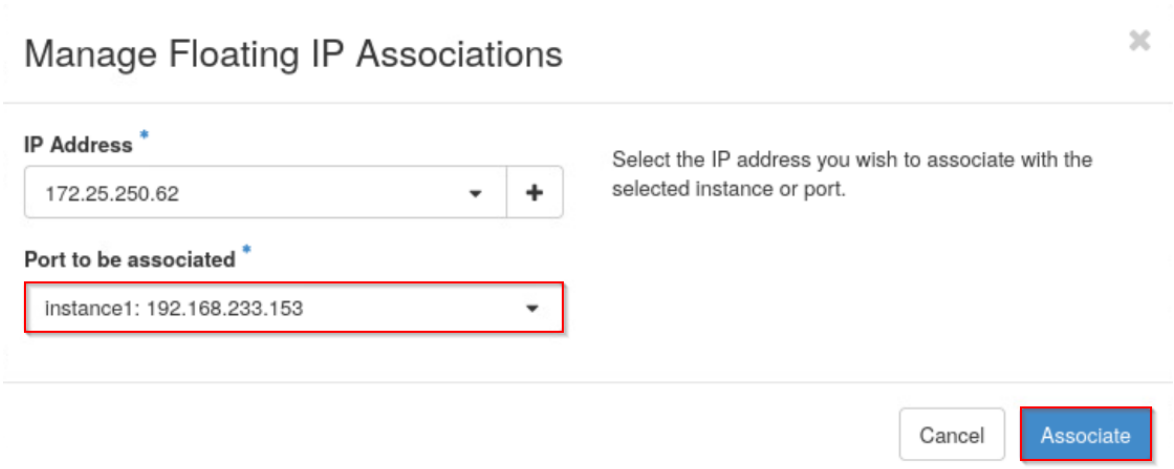
3.6. Click **Associate** in the row of the floating IP address.



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 its floating IP address. At this point, it might seem like the instance should be accessible from a network outside the OpenStack environment. This is a reasonable assumption because the router is accessible, the instance is connected to it, and a floating IP address has been assigned. However, OpenStack applies a "Deny by Default" security model, which means inbound (ingress) traffic to the instance is blocked unless explicitly allowed by security group rules. We'll configure those rules in the next lab. For now, let's verify that **instance1** is *not* reachable. Open a terminal window (if you haven't already), and 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.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Sat Jun 28 14:20:04 2025 from 192.168.1.21
ubuntu@devstack:~$
```

3.9. Use the **ping** command on the floating IP address that was associated with **instance1** in step 7.

```
ubuntu@devstack:~$ ping -c3 172.25.250.62
```

```
ubuntu@devstack:~$ ping -c3 172.25.250.62
PING 172.25.250.62 (172.25.250.62) 56(84) bytes of data.
From 172.25.250.20 icmp_seq=1 Destination Host Unreachable
From 172.25.250.20 icmp_seq=2 Destination Host Unreachable
From 172.25.250.20 icmp_seq=3 Destination Host Unreachable

--- 172.25.250.62 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2036ms
pipe 3
ubuntu@devstack:~$
```

Note

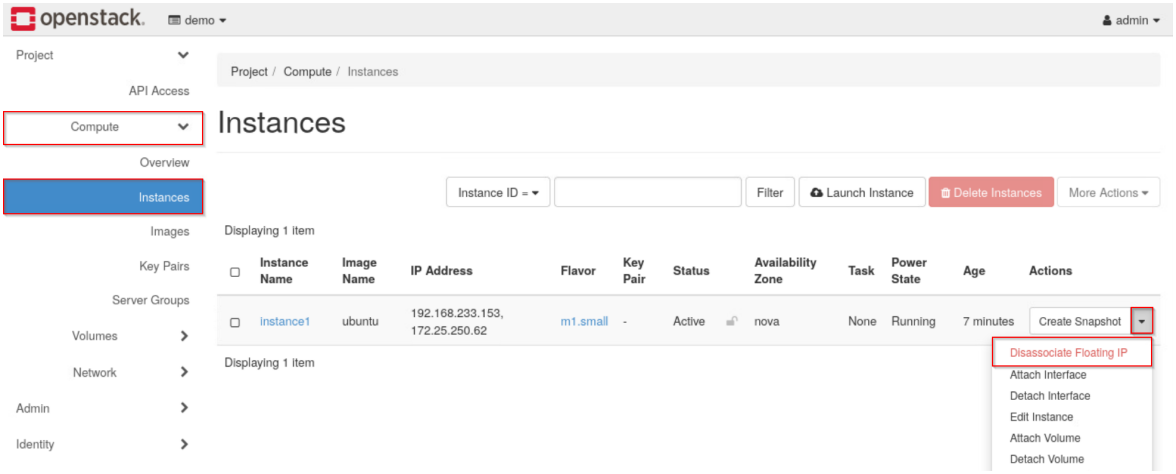
You should not receive any ping replies. Instead, the output of the command should inform you that there was 100% packet loss. This confirms that while the network is configured correctly, the instance is still protected by default security group rules that block incoming traffic.

3.10. Exit the SSH session.

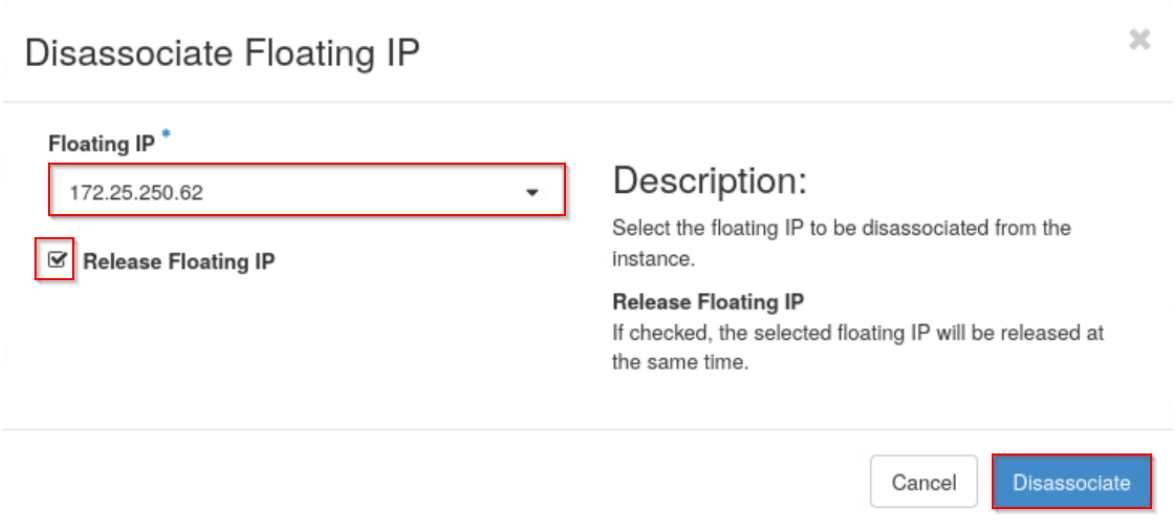
```
ubuntu@devstack:~$ exit
```

```
ubuntu@devstack:~$ exit
logout
Connection to 192.168.1.20 closed.
[ubuntu@workstation (keystone-admin)]:~$
```

3.11. We are now finished with this floating IP address. Return to the web browser. 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.



3.12. 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.

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

3.14. 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          | 2025-06-28T14:31:58Z                 |
| description         |                                      |
| fixed_ip_address    | None                                 |
| floating_ip_address | 172.25.250.75                        |
| floating_network_id | acdc9bc2-56a3-466e-8d27-141c8f71ae99 |
| id                  | c64add8f-8b1e-4043-b398-c544969a0a93 |
| 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          | 2025-06-28T14:31:58Z                 |
+---------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

3.15. Notice that the previous command generated a random floating IP address within the allocation pool. You can use the **–floating-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 HTTP exception.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip list
+--------------+---------------------+------------------+------+------------------+---------------+
| ID           | Floating IP Address | Fixed IP Address | Port | Floating Network | Project       |
+--------------+---------------------+------------------+------+------------------+---------------+
| c64add8f-8b  | 172.25.250.75       | None             | None | acdc9bc2-56a3    | 39e851b14f864 |
| 1e-4043-b39  |                     |                  |      | -466e-8d27-141c8 | 573aad60582c3 |
| 8-c544969a0  |                     |                  |      | f71ae99          | 5e40dc        |
| a93          |                     |                  |      |                  |               |
+--------------+---------------------+------------------+------+------------------+---------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

This command does not properly fit the width of its output until you expand or maximize your terminal window.

Tip

Because this command outputs several IDs, appending arguments such as **-c "Floating IP Address" -c "Fixed IP Address"** to output only the columns you need can make the output easier to read.

3.16. Create the floating IP address **172.25.250.80**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip create \
> --floating-ip-address 172.25.250.80 \
> extern-net2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip create \
> --floating-ip-address 172.25.250.80 \
> extern-net2
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| created_at          | 2025-06-28T14:38:29Z                 |
| description         |                                      |
| fixed_ip_address    | None                                 |
| floating_ip_address | 172.25.250.80                        |
| floating_network_id | acdc9bc2-56a3-466e-8d27-141c8f71ae99 |
| id                  | fcdbfa0a-df36-4cef-89d1-40e67af8e99c |
| name                | 172.25.250.80                        |
| port_id             | None                                 |
| project_id          | 39e851b14f864573aad60582c35e40dc     |
| qos_policy_id       | None                                 |
| revision_number     | 0                                    |
| router_id           | None                                 |
| status              | DOWN                                 |
| subnet_id           | None                                 |
| updated_at          | 2025-06-28T14:38:29Z                 |
+---------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

3.17. Try creating the same floating IP address again. This time, it should return an HTTP exception.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip create \
> --floating-ip-address 172.25.250.80 \
> extern-net2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip create \
> --floating-ip-address 172.25.250.80 \
> extern-net2
Error while executing command: HttpException: Unknown error, {"NeutronError": {"
type": "IpAddressAlreadyAllocated", "message": "IP address 172.25.250.80 already
 allocated in subnet e320bd2f-d0d2-46ba-832a-286ed3e2841c", "detail": ""}}
[ubuntu@workstation (keystone-admin)]:~$
```

3.18. Associate this floating IP address with **instance1**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server add floating ip \
> instance1 \
> 172.25.250.80
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server add floating ip \
> instance1 \
> 172.25.250.80
[ubuntu@workstation (keystone-admin)]:~$
```

3.19. List the details of **instance1** to verify that the floating IP address was attached. The **Networks** column should list both the internal and floating IP address of the instance.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server list
+------------------+-----------+--------+------------------+--------+----------+
| ID               | Name      | Status | Networks         | Image  | Flavor   |
+------------------+-----------+--------+------------------+--------+----------+
| 693c9a39-5469-44 | instance1 | ACTIVE | shared=192.168.2 | ubuntu | m1.small |
| e9-a5c1-99061286 |           |        | 33.38,           |        |          |
| dab0             |           |        | 172.25.250.80    |        |          |
+------------------+-----------+--------+------------------+--------+----------+
[ubuntu@workstation (keystone-admin)]:~$
```

3.20. We are now finished with this floating IP address, so it can be removed from the instance and deleted. Remove the floating IP address from **instance1**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip remove \
> instance1 \
> 172.25.250.80
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server remove floating ip \
> instance1 \
> 172.25.250.80
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

This command is equivalent to clicking **Disassociate** in the Horizon Dashboard, and it is useful when you want to reuse the IP address for something else. However, a floating IP address can be deleted without first removing it from the instance.

3.21. When a floating IP address is removed from an instance, it still exists and is available to add to another instance. List the available floating IP addresses to confirm this.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip list
+--------------+---------------------+------------------+------+------------------+---------------+
| ID           | Floating IP Address | Fixed IP Address | Port | Floating Network | Project       |
+--------------+---------------------+------------------+------+------------------+---------------+
| c64add8f-8b  | 172.25.250.75       | None             | None | acdc9bc2-56a3    | 39e851b14f864 |
| 1e-4043-b39  |                     |                  |      | -466e-8d27-141c8 | 573aad60582c3 |
| 8-c544969a0  |                     |                  |      | f71ae99          | 5e40dc        |
| a93          |                     |                  |      |                  |               |
| fcdbfa0a-    | 172.25.250.80       | None             | None | acdc9bc2-56a3    | 39e851b14f864 |
| df36-4cef-8  |                     |                  |      | -466e-8d27-141c8 | 573aad60582c3 |
| 9d1-40e67af  |                     |                  |      | f71ae99          | 5e40dc        |
| 8e99c        |                     |                  |      |                  |               |
+--------------+---------------------+------------------+------+------------------+---------------+
[ubuntu@workstation (keystone-admin)]:~$
```

3.22. Delete the floating IP address **172.25.250.80**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip delete \
> 172.25.250.80
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip delete \
> 172.25.250.80
[ubuntu@workstation (keystone-admin)]:~$
```

3.23. One floating IP address we originally created at the beginning of this section still exists. Associate this address 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.

3.24. Verify that the floating IP address was added to the instance.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server list
+--------------------+-----------+--------+--------------------+--------+----------+
| ID                 | Name      | Status | Networks           | Image  | Flavor   |
+--------------------+-----------+--------+--------------------+--------+----------+
| 693c9a39-5469-44   | instance1 | ACTIVE | shared=192.168.2   | ubuntu | m1.small |
| e9-a5c1-99061286   |           |        | 33.38,             |        |          |
| dab0               |           |        | 172.25.250.75      |        |          |
+--------------------+-----------+--------+--------------------+--------+----------+
[ubuntu@workstation (keystone-admin)]:~$
```

3.25. 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
```

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

3.26. Verify that the instance was deleted.

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

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

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

3.27. Verify that the floating IP address still exists and that it has no fixed IP address (it is not associated with an instance).

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip list
+------------+---------------------+------------------+------+------------------+--------------+
| ID         | Floating IP Address | Fixed IP Address | Port | Floating Network | Project      |
+------------+---------------------+------------------+------+------------------+--------------+
| 2feb2ef3   | 172.25.250.75       | None             | None | acdc9bc2-56a3    | 39e851b14f864 |
| -54cf-4f41 |                     |                  |      | -466e-8d27-141c8 | 573aad60582c3 |
| -ad3a-9bbbc |                    |                  |      | f71ae99          | 5e40dc       |
| a16309a    |                     |                  |      |                  |              |
+------------+---------------------+------------------+------+------------------+--------------+
[ubuntu@workstation (keystone-admin)]:~$
```

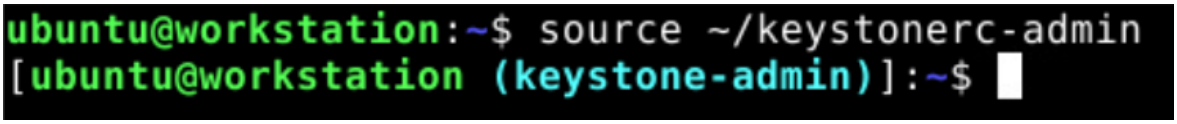
3.28. Leave the terminal window open and continue to the next task.

4 Deleting Routers and External Networks from the CLI

Earlier in the lab, you deleted a router by manually removing its connected subnets, since you already knew their names. While that approach works in simple cases, it doesn't scale well to routers with many interfaces or when subnet names aren't known in advance. In this task, you will use the *OpenStack Unified CLI* to clean up the environment by deleting the router and external network you previously created. This time, you'll use a more flexible and automated approach that works even when subnet names are unknown. You will also learn a few useful tricks for working with commands that require resource IDs as arguments, which will be helpful when writing cleanup scripts or handling more complex environments.

4.1. 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
```



4.2. When working from the Horizon Dashboard, a network cannot be deleted if it is connected to a router. Although the command line allows them to be deleted in either order, we will still delete the router first. Begin by viewing the details of **router2**.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router show router2
+-------------------------+-----------------------------------------------------+
| Field                   | Value                                               |
+-------------------------+-----------------------------------------------------+
| admin_state_up          | UP                                                  |
| availability_zone_hints |                                                     |
| availability_zones      |                                                     |
| created_at              | 2025-07-02T17:13:05Z                                |
| description             |                                                     |
| distributed             | False                                               |
| external_gateway_info   | None                                                |
| flavor_id               | None                                                |
| ha                      | False                                               |
| id                      | 9bd4dba7-fdd0-4eae-a0ef-c84628323e72                |
| interfaces_info         | [{"subnet_id": "ab9d42da-bf78-43dd-                 |
|                         | 9ec4-e1aa5cd74e5d", "ip_address":                   |
|                         | "172.25.250.254", "port_id":                        |
|                         | "220b616e-4502-45c7-b0c5-cdc7c2afef90"},            |
|                         | {"subnet_id": "7e456257-76e5-4cfc-bf3f-             |
|                         | b2a3876dba40", "ip_address": "192.168.233.1",       |
|                         | "port_id": "2fb8ad7d-a8c9-4e3a-964e-                |
|                         | 17bb433d10ff"}]                                     |
| name                    | router2                                             |
| project_id              | 39e851b14f864573aad60582c35e40dc                    |
| revision_number         | 10                                                  |
| routes                  |                                                     |
| status                  | ACTIVE                                              |
| tags                    |                                                     |
| updated_at              | 2025-07-02T17:31:43Z                                |
+-------------------------+-----------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

4.3. From the CLI, a router's subnets and interfaces, including its external gateway, must first be cleared before deleting the router. Unset the external gateway of **router2**.

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

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

4.4. Next, each of the router's interfaces must be deleted. This time, we will specify the interfaces by their IDs. To avoid copying and pasting the ID values, we will store them in a variable and delete them at the same time. First, list the router's interface IDs.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack port list \
> -c ID \
> -f value \
> --router router2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack port list \
> -c ID \
> -f value \
> --router router2
220b616e-4502-45c7-b0c5-cdc7c2afef90
2fb8ad7d-a8c9-4e3a-964e-17bb433d10ff
[ubuntu@workstation (keystone-admin)]:~$
```

Note

The **-f value** argument specifies that rather than outputting the result in a table format, we want just the value. There are a few other output options, such as **-f json**, but we will not need any other options in these labs.

4.5. Now, assign the output of the previous step to a variable called **ports**.

```
[ubuntu@workstation (keystone-admin)]:~$ ports=$(!!)
```

```
[ubuntu@workstation (keystone-admin)]:~$ ports=$(!!)
ports=$(openstack port list -c ID -f value --router router2)
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

Make sure there are no spaces around the equal sign when assigning a value to a variable.

Note

The **$(...)** syntax captures the output of a command, and **!!** re-executes the immediately preceding command. In this case, we could have also used

```
ports=$(openstack router port list --router router2 -c ID -f value)
```

However, this consumes the output of the command and does not print it unless you use the **echo** command as well.

4.6. Print the value of the **ports** variable to make sure it is storing the ID values. The **$** symbol is used to access the value of a variable.

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

```
[ubuntu@workstation (keystone-admin)]:~$ echo $ports
220b616e-4502-45c7-b0c5-cdc7c2afef90 2fb8ad7d-a8c9-4e3a-964e-17bb433d10ff
[ubuntu@workstation (keystone-admin)]:~$
```

Note

Notice that the IDs are separated by a space. This is exactly what we want, since that is what the **for** loop we use in the next step expects.

4.7. Unfortunately, because most OpenStack commands cannot accept a list of arguments, removing multiple ports at once requires a **for** loop. With this loop, we will access each of the port IDs stored in the **ports** variable, and we will run the command for each ID value. Delete the interfaces of **router2** by using the **ports** variable.

```
[ubuntu@workstation (keystone-admin)]:~$ for port in $ports; do \
> openstack router remove port router2 $port; \
> done
```

```
[ubuntu@workstation (keystone-admin)]:~$ for port in $ports; do \
> openstack router remove port router2 $port; \
> done
[ubuntu@workstation (keystone-admin)]:~$
```

Note

The syntax of a **for** loop is

```
for item in $list; do <command> $item; done
```

In this syntax, **list** is a variable containing multiple values. The **for** loop runs the command once for each item. In our case, it will go through each port ID stored in the **ports** variable, then delete it from the router. If **ports** contains three IDs, the loop runs this command three times—once per ID:

```
openstack router remove port router2 <ID1>
openstack router remove port router2 <ID2>
openstack router remove port router2 <ID3>
```

Tip

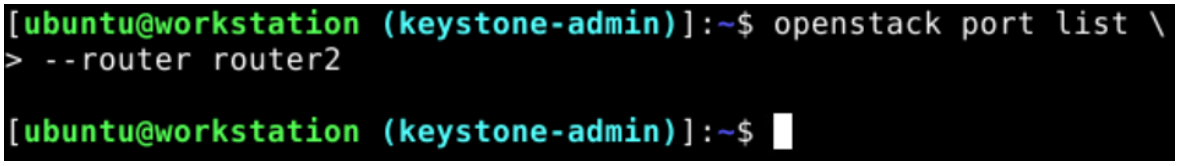
If you know the names of a router's subnets, they can also be used to delete a router's interfaces with the command

```
openstack router remove subnet <subnet-name-or-id>
```

In this case, we could have used **shared-subnet** and **extern-subnet2** since we knew the names. However, the method outlined above is more general, and it could even be made into a script to automate router deletion if it becomes a common task.

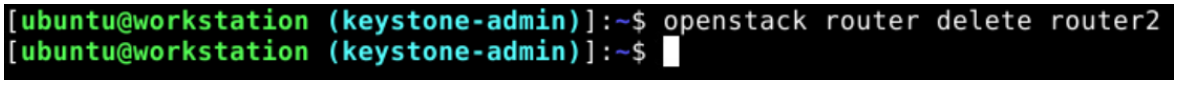
4.8. Verify that the interfaces of **router2** were deleted.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack port list \
> --router router2
```



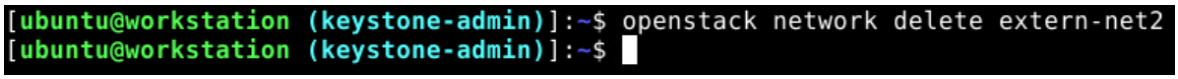
4.9. **router2** can now be deleted.

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



4.10. The **external** network can also be deleted.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network delete extern-net2
```



Note

You've now used the CLI to fully delete a router and its associated external network—even without knowing subnet names. This approach can be adapted into scripts and is essential for managing more complex OpenStack environments.

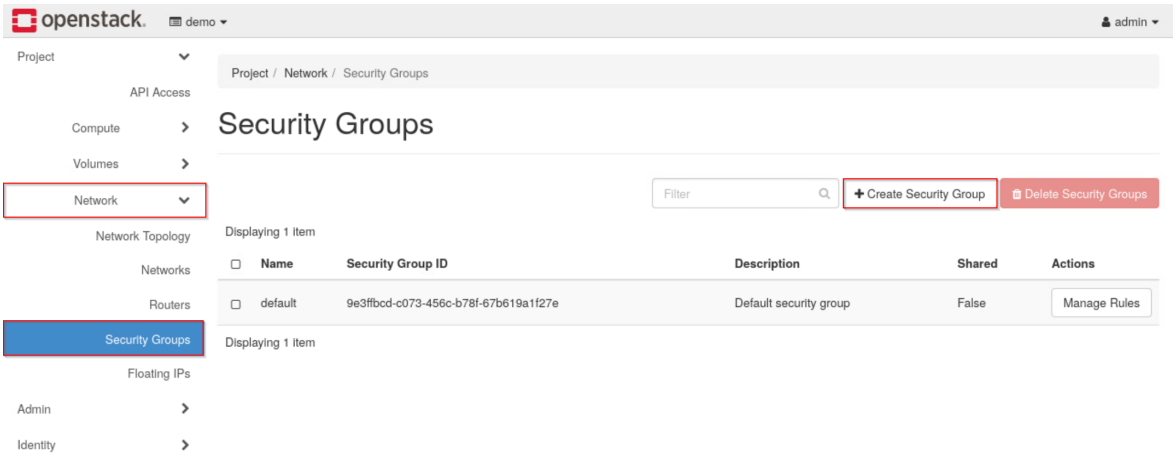
4.11. Leave the terminal window open, and continue to the next step.

5 Defining Security Groups

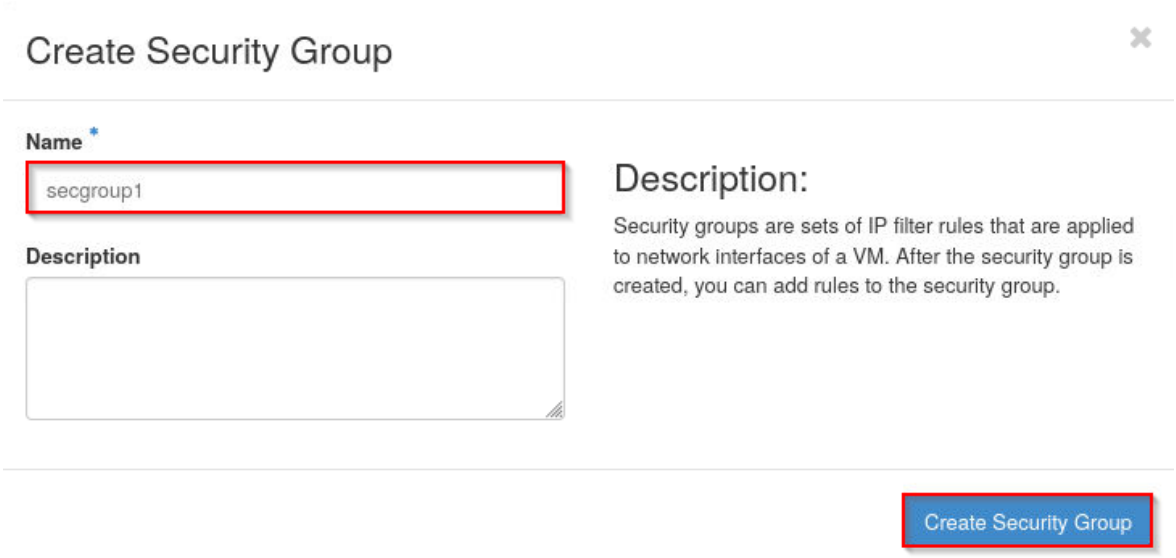
In this task, you will use the *Horizon Dashboard* and *OpenStack Unified CLI* to manage security groups for OpenStack instances. Security groups function like virtual firewalls, allowing you to define rules that allow or deny specific types of network traffic. Modifying the default security group settings is essential to enable communication with external instances from outside the OpenStack environment. In this lab, we are concerned with two types of traffic in particular: ICMP to allow the use of the **ping** command, and SSH to enable remote login from an external network.

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

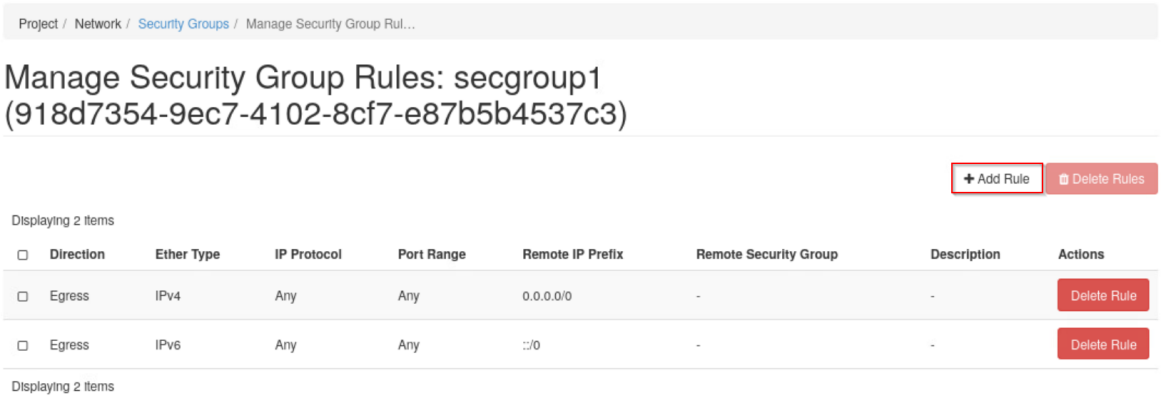
5.2. Select the **demo** project. Navigate to **Network** > **Security Groups** and click **Create Security Group**.



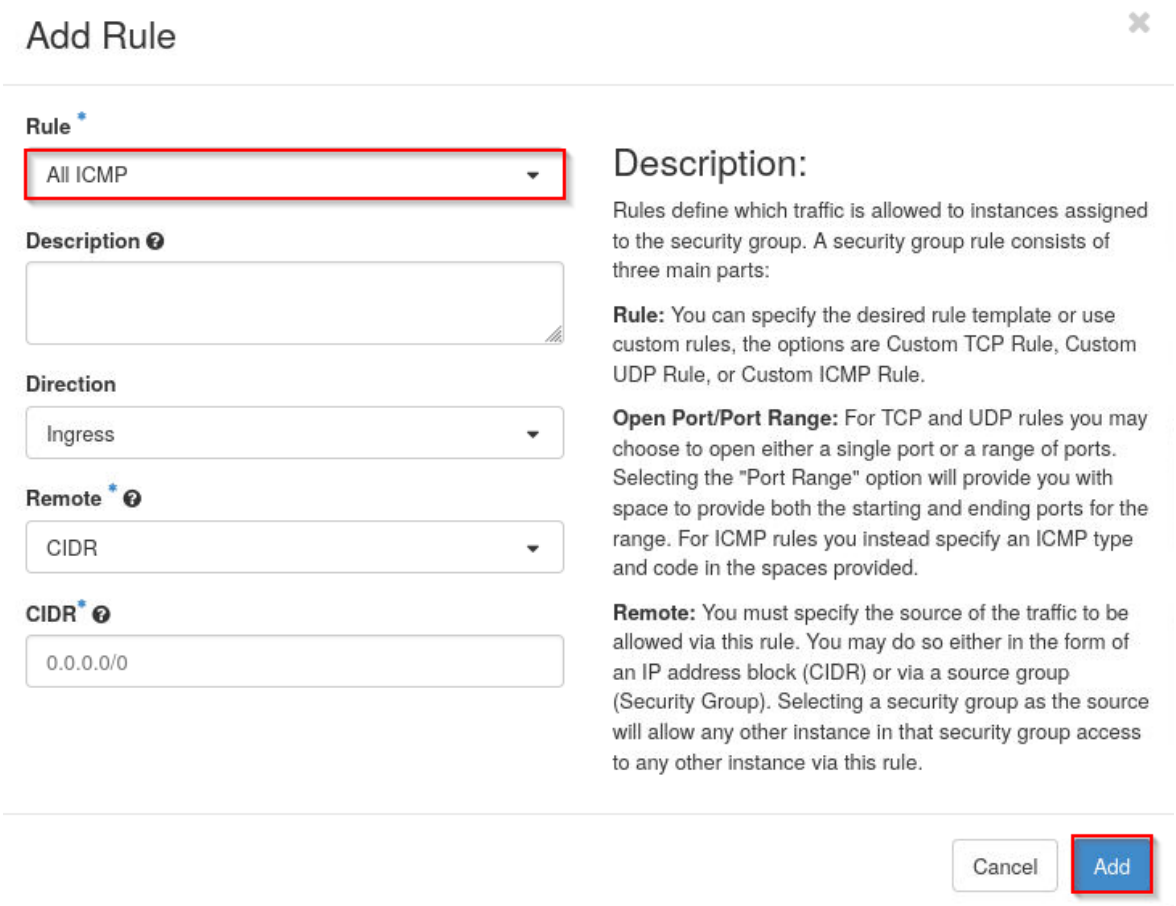
5.3. Enter **secgroup1** into the *Name* field and click **Create Security Group**.



5.4. After creating the security group, you should be redirected to its rules page. 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 all egress (outgoing) traffic. No ingress rules are defined, so all incoming traffic is denied by default. Click **Add Rule** to add a new rule in the security group.

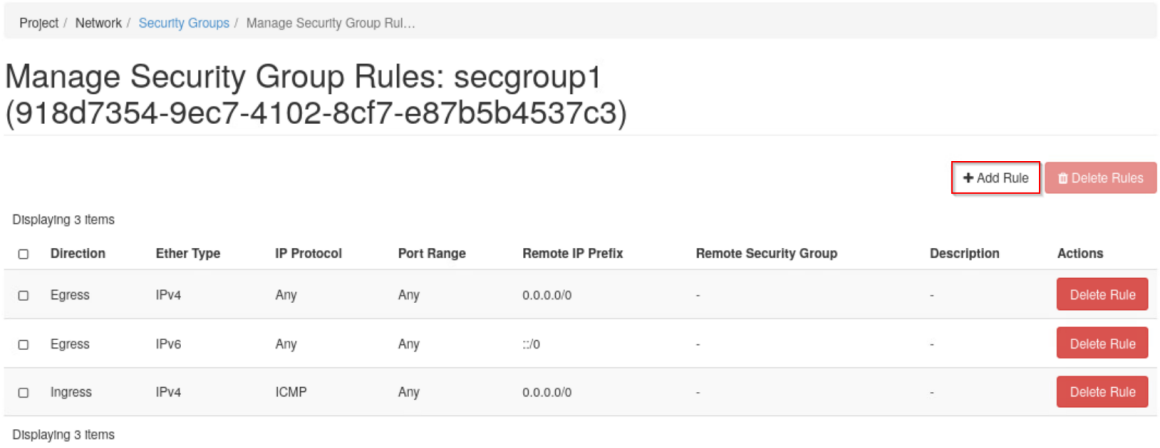


5.5. Select **All ICMP** from the *Rule* dropdown and click **Add**. This allows ICMP traffic, including the **ping** command, to reach instances in this security group.

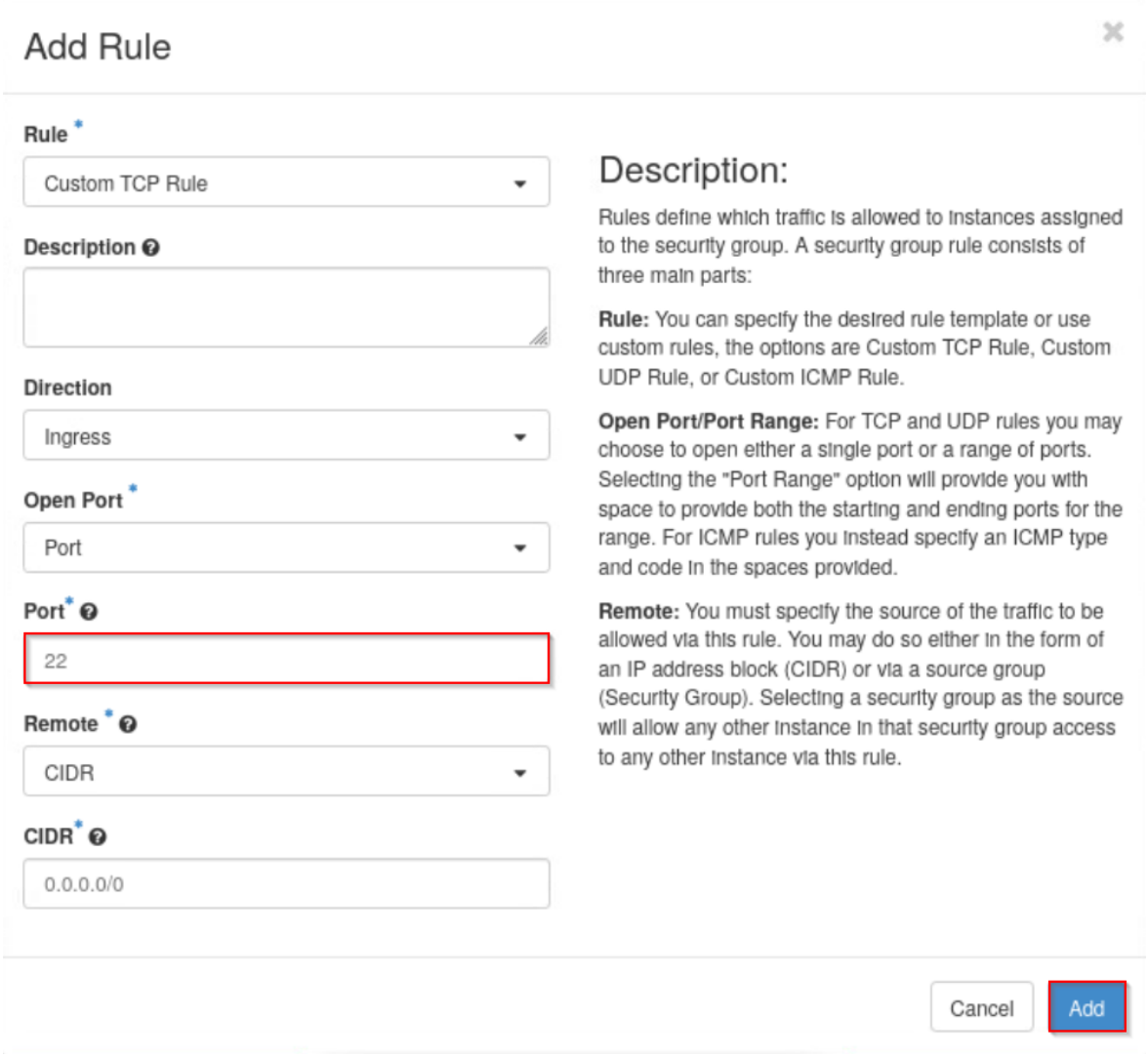


> **Note**
>
> By default, *Direction* is set to **Ingress** and *CIDR* is set to **0.0.0.0/0**. **Ingress** specifies incoming traffic, and **0.0.0.0/0** specifies that the traffic is accepted from any IP address.

5.6. Click **Add Rule** again.



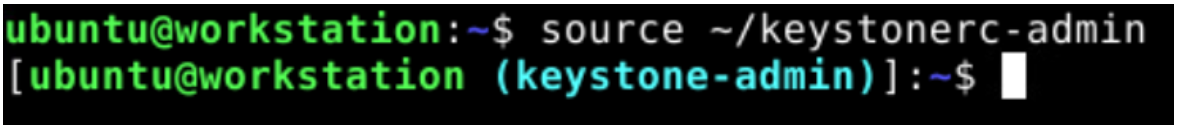
5.7. Now, we will create a rule to allow SSH ingress traffic. Since SSH works over TCP, leave *Rule* as **Custom TCP Rule**. Under *Port*, enter **22**, which is the default SSH port. Click **Add** to add the rule.



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

5.9. 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
```



5.10. Before creating or modifying any security groups or rules, list the existing security groups to see what is already configured.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group list
+--------------------+-----------+---------------------+----------------------+
| ID                 | Name      | Description         | Project              |
+--------------------+-----------+---------------------+----------------------+
| 2f0f5133-8396-45ea-| default   | Default security    | eb2dcd08d8ae46ffac3f |
| a4de-61945d79ed2e  |           | group               | 16c3973ef61d         |
| 62dafb67-e7fd-44d6-| default   | Default security    | 39e851b14f864573aad6 |
| bf87-f4701dd66875  |           | group               | 0582c35e40dc         |
| 918d7354-9ec7-4102-| secgroup1 |                     | 39e851b14f864573aad6 |
| 8cf7-e87b5b4537c3  |           |                     | 0582c35e40dc         |
+--------------------+-----------+---------------------+----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

5.11. Now, we will recreate the **secgroup1** 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
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup1
+--------------------------------------+-------------+-----------+------------+-----------------------+
| ID                                   | IP Protocol | IP Range  | Port Range | Remote Security Group |
+--------------------------------------+-------------+-----------+------------+-----------------------+
| 022a7e4f-41ce-4c37-9764-e22733a5bc19 | None        | None      |            | None                  |
| 8b0035c8-f81e-451d-bf0a-dd258ebca9f4 | icmp        | 0.0.0.0/0 |            | None                  |
| 9ba01e49-f422-43e2-b731-8e25f58bc428 | tcp         | 0.0.0.0/0 | 22:22      | None                  |
| bce3af7e-2cee-48a3-99d2-3d05c709a159 | None        | None      |            | None                  |
+--------------------------------------+-------------+-----------+------------+-----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

Since we want to copy the ID value, we do not want the output to fit the width of the terminal window, which would wrap the ID across multiple lines and prevent copying. To prevent this, maximize the terminal window before running this command.

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**.

5.12. Use the ID for the ICMP rule to delete that rule. Note that you do not have to list **secgroup1** in this command because IDs in OpenStack are *globally unique* within a deployment.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule delete \
> fb6707a2-ee35-417f-a3c1-947da634b206
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule delete \
> 8b0035c8-f81e-451d-bf0a-dd258ebca9f4
[ubuntu@workstation (keystone-admin)]:~$
```

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**.

5.13. 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
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup1
+--------------------------------------+-------------+-----------+-----------+-----------------------+
| ID                                   | IP Protocol | IP Range  | Port Range | Remote Security Group |
+--------------------------------------+-------------+-----------+-----------+-----------------------+
| 022a7e4f-41ce-4c37-9764-e22733a5bc19 | None        | None      |           | None                  |
| 9ba01e49-f422-43e2-b731-8e25f58bc428 | tcp         | 0.0.0.0/0 | 22:22     | None                  |
| bce3af7e-2cee-48a3-99d2-3d05c709a159 | None        | None      |           | None                  |
+--------------------------------------+-------------+-----------+-----------+-----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

5.14. 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)]:~$
```

5.15. Create the **secgroup2** security group.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group create \
> secgroup2
+-----------------+-------------------------------------------------------------+
| Field           | Value                                                       |
+-----------------+-------------------------------------------------------------+
| created_at      | 2025-06-28T15:52:22Z                                        |
| description     | secgroup2                                                   |
| id              | d4792861-920e-4dd6-bdd1-e9ea3b5f6d6a                        |
| name            | secgroup2                                                   |
| project_id      | 39e851b14f864573aad60582c35e40dc                            |
| revision_number | 1                                                           |
| rules           | created_at='2025-06-28T15:52:22Z', direction='egress',      |
|                 | ethertype='IPv6',                                           |
|                 | id='4ca422bf-c170-4159-b1e6-329c949d01e4',                  |
|                 | standard_attr_id='79', updated_at='2025-06-28T15:52:22Z'    |
|                 | created_at='2025-06-28T15:52:22Z', direction='egress',      |
|                 | ethertype='IPv4',                                           |
|                 | id='c409c480-d296-4009-abf9-3e01c3b2c6ca',                  |
|                 | standard_attr_id='80', updated_at='2025-06-28T15:52:22Z'    |
| updated_at      | 2025-06-28T15:52:22Z                                        |
+-----------------+-------------------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

5.16. 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 |
+--------------------------------------+-------------+----------+-----------+-----------------------+
| 4ca422bf-c170-4159-b1e6-329c949d01e4 | None        | None     |           | None                  |
| c409c480-d296-4009-abf9-3e01c3b2c6ca | 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.

5.17. 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        | 2025-06-28T16:05:07Z                 |
| description       |                                      |
| direction         | ingress                              |
| ether_type        | IPv4                                 |
| id                | 822e6305-b7a4-4df6-8f7b-74d117171381 |
| 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 | d4792861-920e-4dd6-bdd1-e9ea3b5f6d6a |
| updated_at        | 2025-06-28T16:05:07Z                 |
+-------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Note

If no additional 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.

5.18. 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
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup2
+--------------------------------------+-------------+-----------+-----------+-----------------------+
| ID                                   | IP Protocol | IP Range  | Port Range | Remote Security Group |
+--------------------------------------+-------------+-----------+-----------+-----------------------+
| 4ca422bf-c170-4159-b1e6-329c949d01e4 | None        | None      |           | None                  |
| 822e6305-b7a4-4df6-8f7b-74d117171381 | icmp        | 0.0.0.0/0 |           | None                  |
| c409c480-d296-4009-abf9-3e01c3b2c6ca | None        | None      |           | None                  |
+--------------------------------------+-------------+-----------+-----------+-----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

5.19. 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        | 2025-06-28T16:07:08Z                 |
| description       |                                      |
| direction         | ingress                              |
| ether_type        | IPv4                                 |
| id                | 3af8f304-cd2c-4e3c-a68a-fa04e3155c94 |
| 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 | d4792861-920e-4dd6-bdd1-e9ea3b5f6d6a |
| updated_at        | 2025-06-28T16:07:08Z                 |
+-------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

5.20. 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
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> secgroup2
+--------------------------------------+-------------+-----------+-----------+-----------------------+
| ID                                   | IP Protocol | IP Range  | Port Range | Remote Security Group |
+--------------------------------------+-------------+-----------+-----------+-----------------------+
| 3af8f304-cd2c-4e3c-a68a-fa04e3155c94 | tcp         | 0.0.0.0/0 | 22:22      | None                  |
| 4ca422bf-c170-4159-b1e6-329c949d01e4 | None        | None      |            | None                  |
| 822e6305-b7a4-4df6-8f7b-74d117171381 | icmp        | 0.0.0.0/0 |            | None                  |
| c409c480-d296-4009-abf9-3e01c3b2c6ca | None        | None      |            | None                  |
+--------------------------------------+-------------+-----------+-----------+-----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

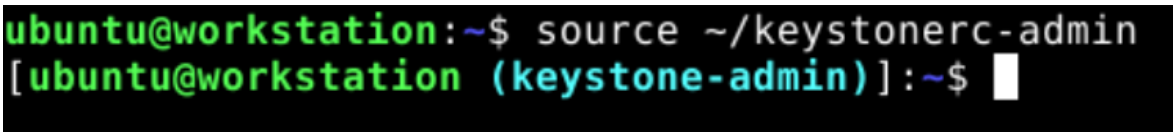
5.21. Leave the terminal window open and continue to the next task.

6 Applying Security Groups to Instances

In order for a security group's rules to apply to instance, the security group must be applied to one of the instance's interfaces. In these labs, instances will only have one interface, so a security group can be thought of as applying to the whole instance. Additionally, an interface may have more than one security group applied. Security groups can be added to an instance when the instance is created, and they can be added, removed, or modified at any time. This section will walk through adding and removing an instance's security groups with both the *OpenStack Unified CLI* and the *Horizon Dashboard*.

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. A security group can be applied to an instance at creation from the command line. Create an instance with the security group **secgroup2** applied to it.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --network shared \
> --security-group secgroup2 \
> instance1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --network shared \
> --security-group secgroup2 \
> 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                           | PTPvFbjoJb8A                         |
| config_drive                        |                                      |
| created                             | 2025-06-28T16:10:49Z                 |
| flavor                              | m1.small (2)                         |
| hostId                              |                                      |
| id                                  | f410ecba-01c0-47d6-b5ef-e991f54cff55 |
| image                               | ubuntu (329d361e-f6dc-               |
|                                     | 4b72-b200-3de0ec230e65)              |
| key_name                            | None                                 |
| name                                | instance1                            |
| progress                            | 0                                    |
| project_id                          | 39e851b14f864573aad60582c35e40dc     |
| properties                          |                                      |
| security_groups                     | name='d4792861-920e-                 |
|                                     | 4dd6-bdd1-e9ea3b5f6d6a'              |
| status                              | BUILD                                |
| updated                             | 2025-06-28T16:10:49Z                 |
| user_id                             | 14f5376f00c04e90b7103dd8d4263040     |
| volumes_attached                    |                                      |
+-------------------------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

6.3. The output of the previous step should have shown the ID of **secgroup2** in the **security_groups** row. To get a result that easier to understand and verify that **secgroup2** is attached to the instance, we can show the details of the instance with a couple extra arguments.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server show \
> -c security_groups \
> instance1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server show \
> -c security_groups \
> instance1
+-----------------+------------------+
| Field           | Value            |
+-----------------+------------------+
| security_groups | name='secgroup2' |
+-----------------+------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

The **-c security_groups** argument specifies that we want only the **security_groups** row in the output.

6.4. Remove **secgroup2** from the instance.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server remove security group \
> instance1 secgroup2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server remove security group \
> instance1 \
> secgroup2
keys: ['name']
[ubuntu@workstation (keystone-admin)]:~$
```

Note

This command may echo the string **keys: ['name']**. Ignore this output; the command still works as intended.

6.5. Verify that the security group is no longer applied to the instance. You should receive an error message saying the column name is not recognized.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server show \
> -c security_groups \
> instance1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server show \
> -c security_groups \
> instance1
No recognized column names in [u'security_groups']. Recognized columns are (u'OS-D
CF:diskConfig', u'OS-EXT-AZ:availability_zone', u'OS-EXT-SRV-ATTR:host', u'OS-EXT-
SRV-ATTR:hypervisor_hostname', u'OS-EXT-SRV-ATTR:instance_name', u'OS-EXT-STS:powe
r_state', u'OS-EXT-STS:task_state', u'OS-EXT-STS:vm_state', u'OS-SRV-USG:launched_
at', u'OS-SRV-USG:terminated_at', u'accessIPv4', u'accessIPv6', u'addresses', u'co
nfig_drive', u'created', u'flavor', u'hostId', u'id', u'image', u'key_name', u'nam
e', u'progress', 'project_id', 'properties', u'status', u'updated', u'user_id', 'v
olumes_attached').
[ubuntu@workstation (keystone-admin)]:~$
```

6.6. A security group can also be added to an instance after the instance is created. Add **secgroup2** back to the instance.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server add security group \
> instance1 secgroup2
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server add security group \
> instance1 \
> secgroup2
keys: ['name']
[ubuntu@workstation (keystone-admin)]:~$
```

Note

This command may echo the string **keys: ['name']**. Ignore this output; the command still works as intended.

6.7. Verify that the security group is once again applied to the instance.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server show \
> -c security_groups \
> instance1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server show \
> -c security_groups \
> instance1
+-----------------+-----------------+
| Field           | Value           |
+-----------------+-----------------+
| security_groups | name='secgroup2' |
+-----------------+-----------------+
[ubuntu@workstation (keystone-admin)]:~$
```

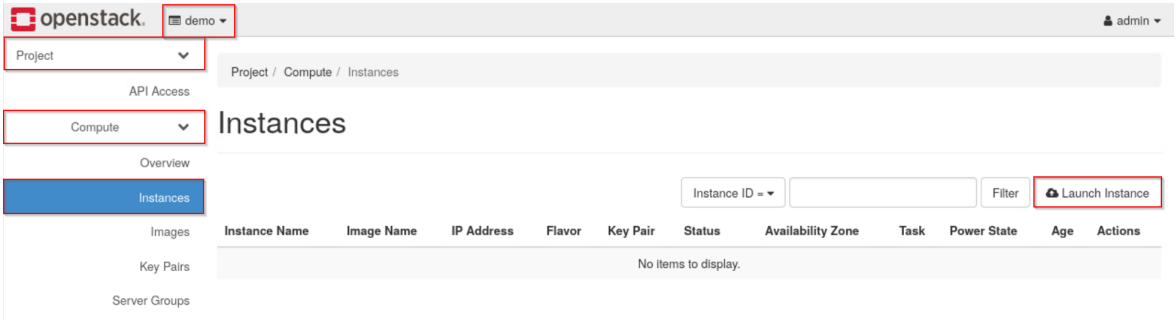
6.8. Delete **instance1**. We will recreate it from the Horizon Dashboard to demonstrate adding a security group to an instance at creation time from the dashboard.

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

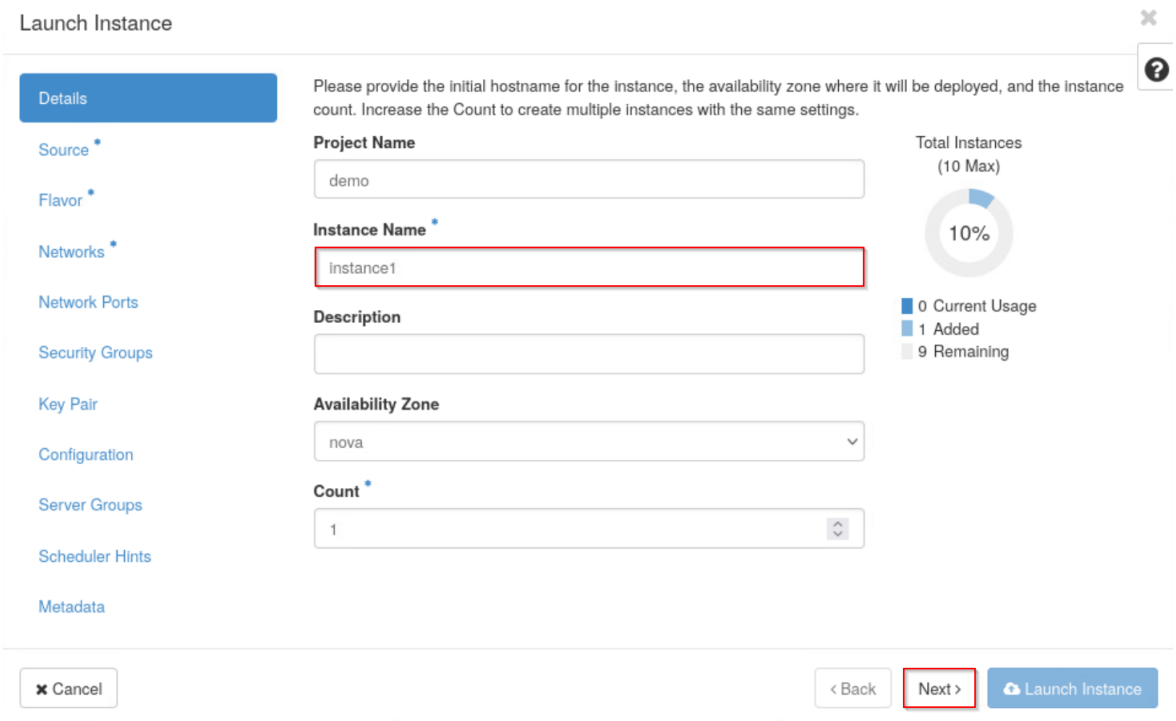
```
[ubuntu@workstation (keystone-admin)]:~$ openstack server delete instance1
[ubuntu@workstation (keystone-admin)]:~$
```

6.9. Leave the terminal window open, and open the web browser. Navigate to **192.168.1.20** and log in to the dashboard as **admin** with the password **secret**.

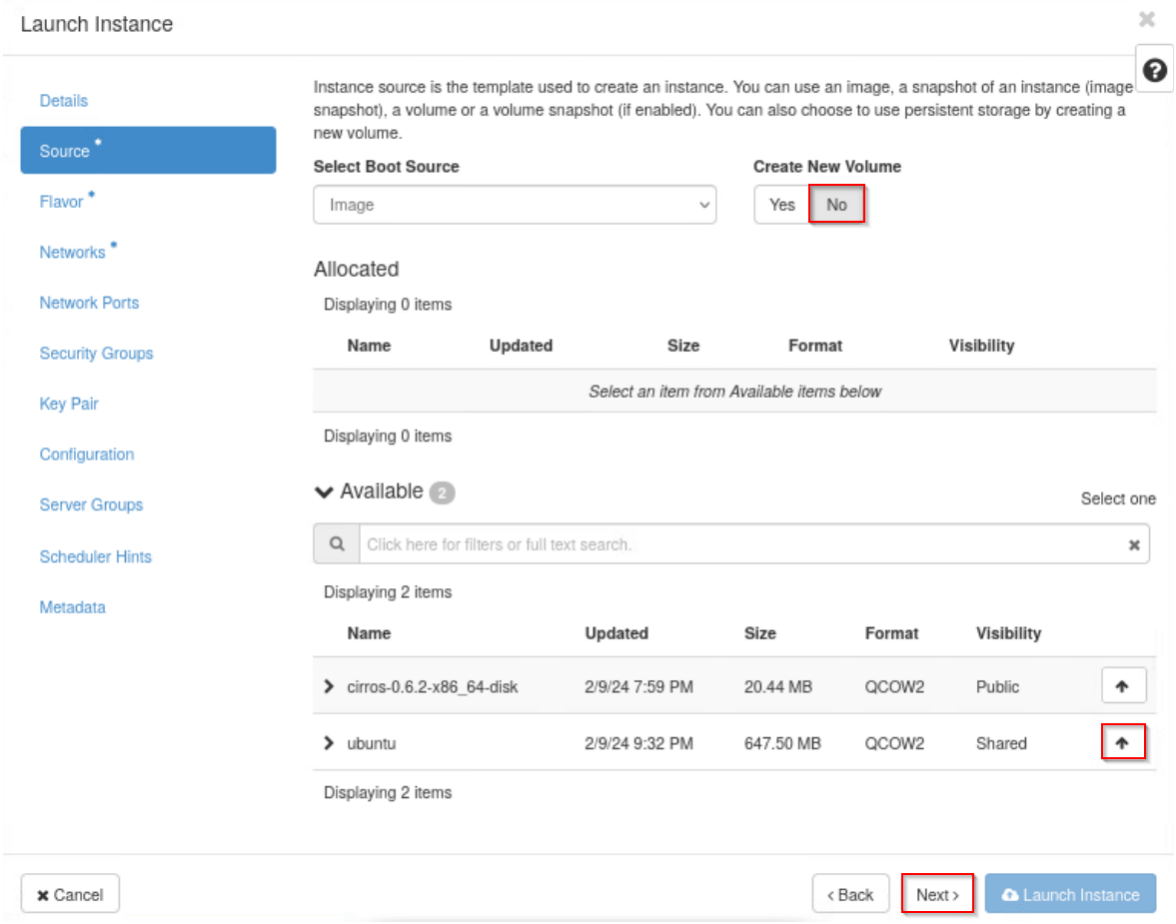
6.10. Select the **demo** project. Navigate to **Project** > **Compute** > **Instances**, and click **Launch Instance**.



6.11. In the *Details* tab, type **instance1** in the *Instance Name* field. Click **Next**.



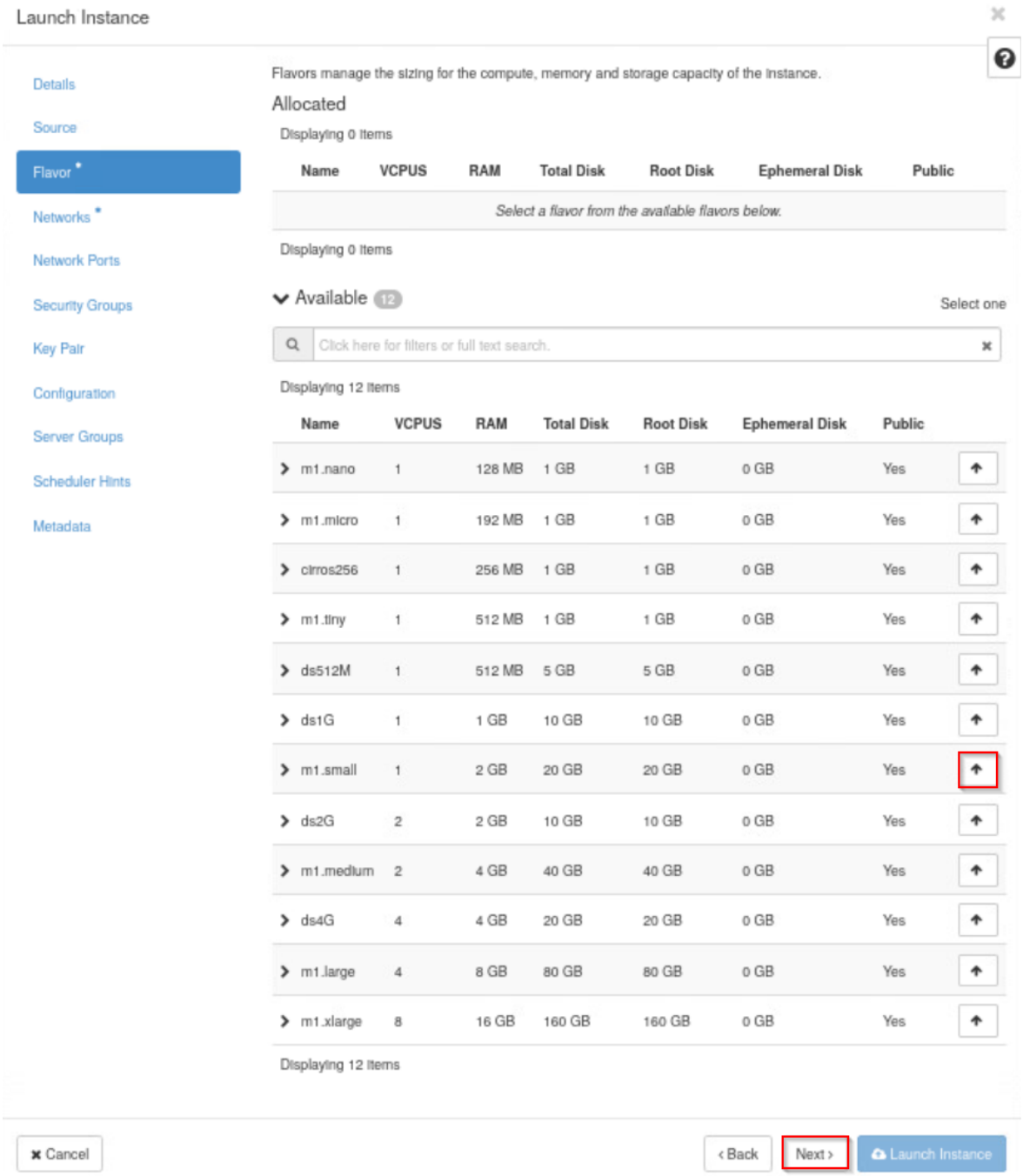
6.12. In the *Source* tab, set *Create New Volume* to **No**, and scroll down (if needed) to select the **ubuntu** image. Click **Next**.



Stop

Before proceeding to the next step, confirm that **ubuntu** appears in the *Allocated* section.

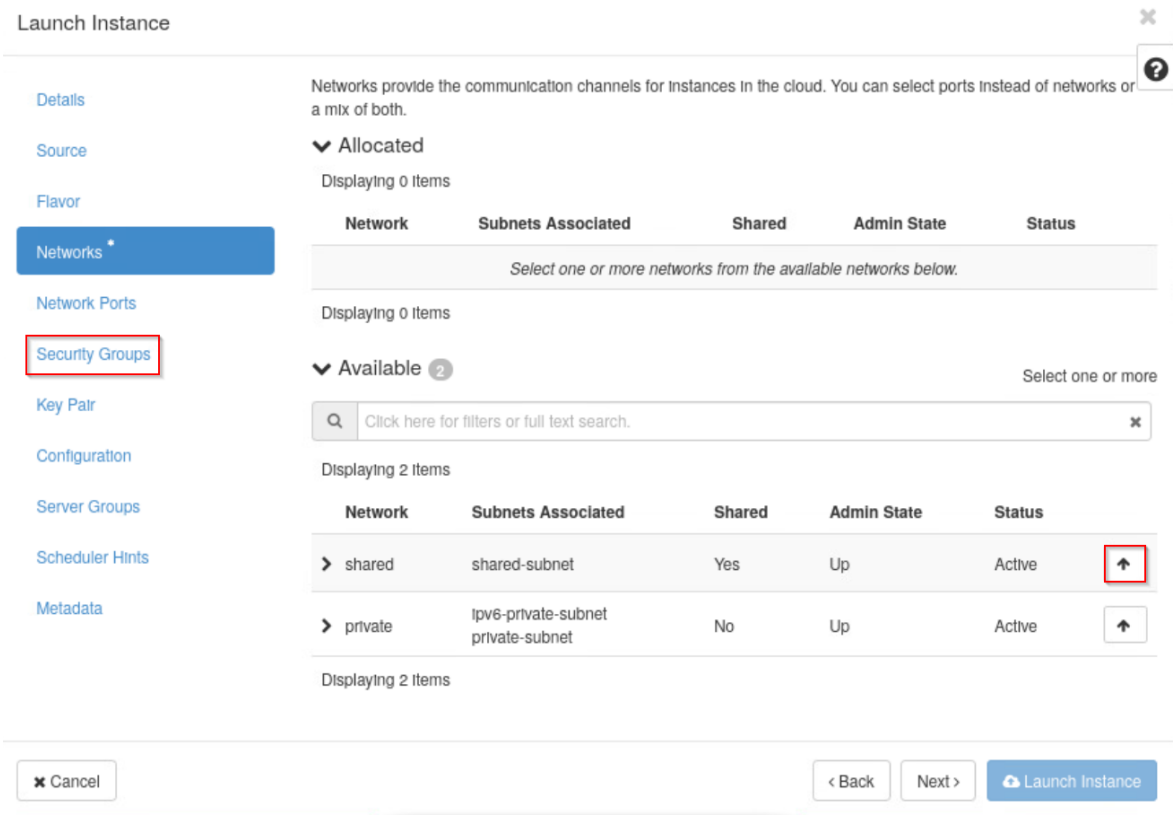
6.13. In the *Flavor* tab, scroll down (if needed) to select the **m1.small** flavor. Click **Next**.



Stop

Before proceeding to the next step, confirm that **m1.small** appears in the *Allocated* section.

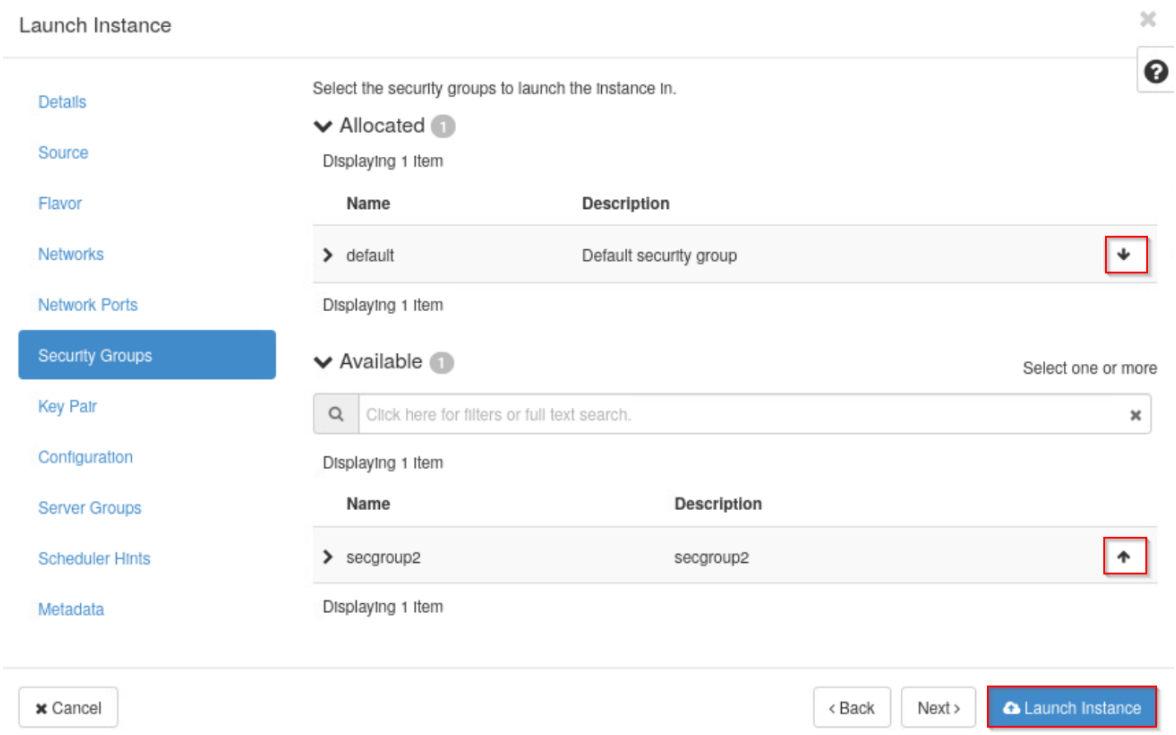
6.14. In the *Networks* tab, select the **shared** network. Navigate to the **Security Groups** tab.



Stop

Before proceeding to the next step, confirm that **shared** appears in the *Allocated* section.

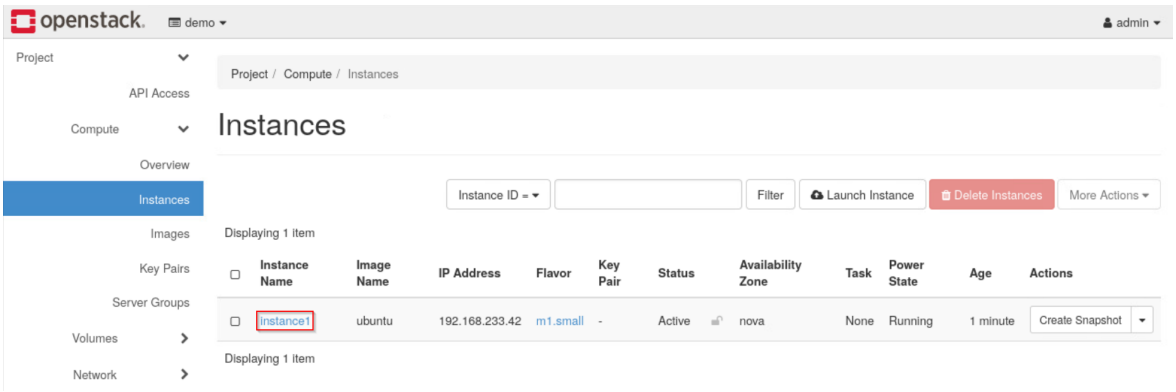
6.15. In the *Security Groups* tab, deselect the **default** security group since we have our own to apply. Scroll down (if needed) to select the **secgroup2** security group. This will apply the security group to all interfaces on the instance. Click **Launch Instance**.



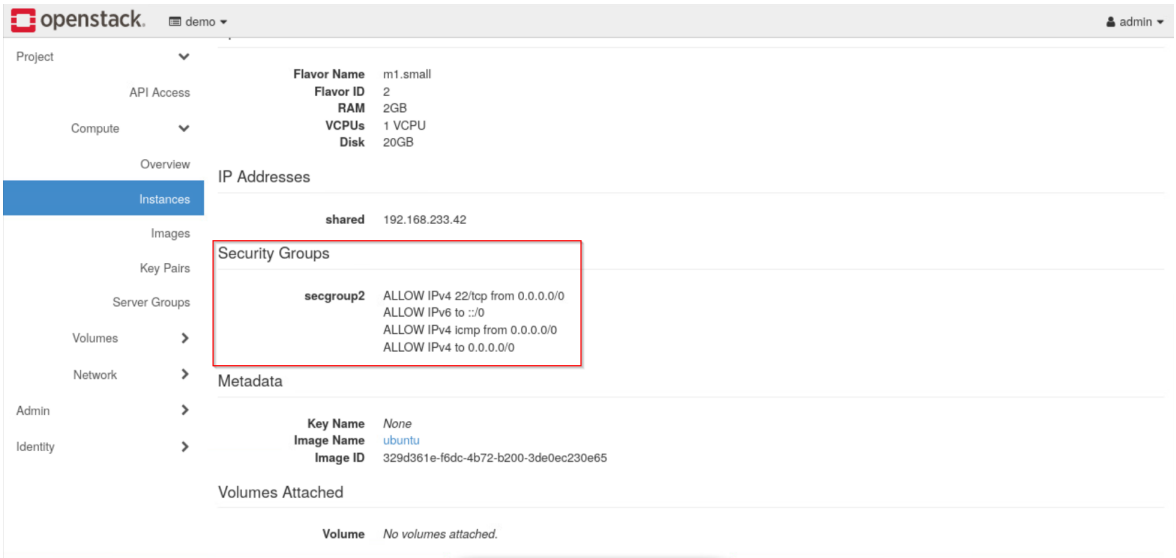
Stop

Before proceeding to the next step, confirm that **secgroup2** appears in the *Allocated* section.

6.16. You should be redirected to the **Project** > **Compute** > **Instances** page. The security groups and rules applied to an instance can be found by clicking the instance's name.



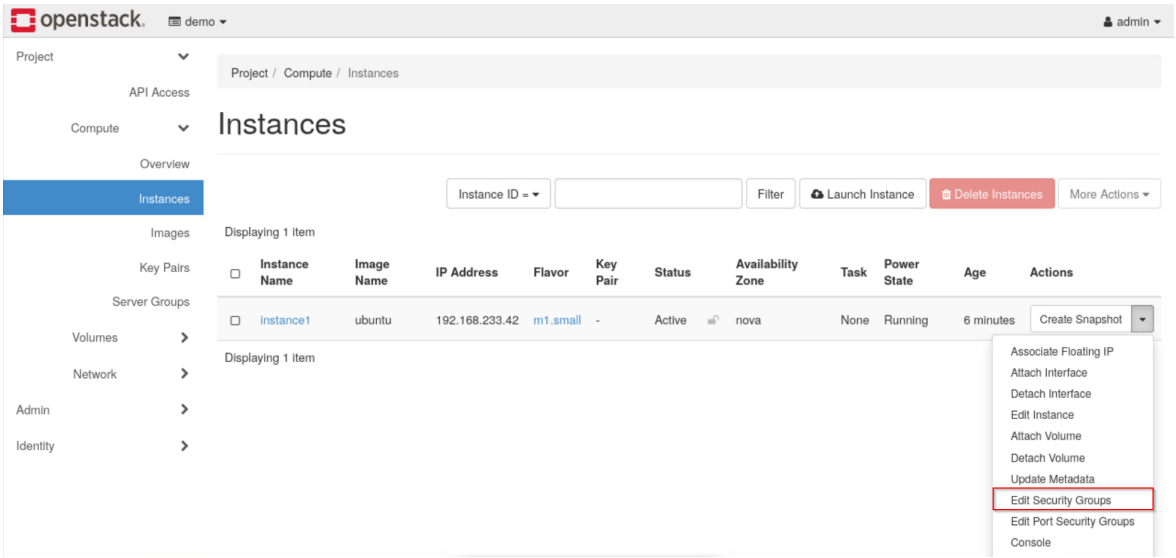
6.17. On the *Overview* tab of the *instance1* page, scroll down to view the *Security Groups* section. In this case, you should see that **secgroup2** allows all IPv4 and IPv6 egress traffic by default, and you should see the two rules we added for ICMP and SSH (TCP port 22).



Note

If no security group is applied to an instance, the *Security Groups* section will simply say "Not available".

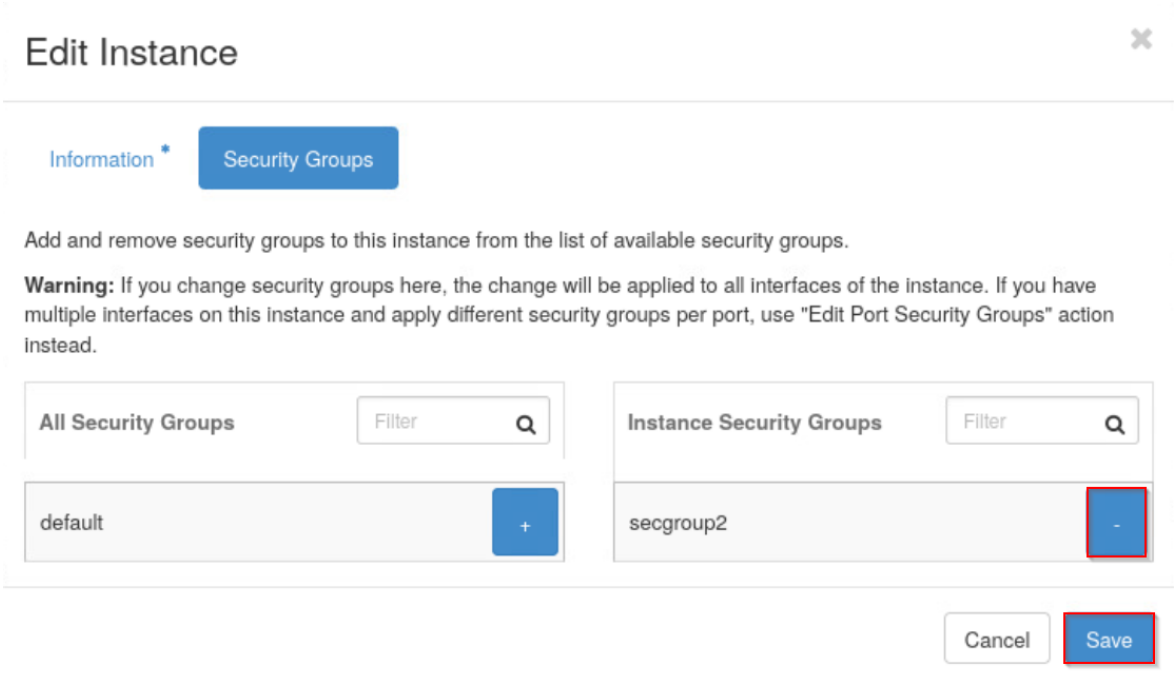
6.18. Navigate back to **Project** > **Compute** > **Instances**. To view and edit the security groups of an instance from the dashboard, click the dropdown next to **Create Snapshot**, and click **Edit Security Groups**.



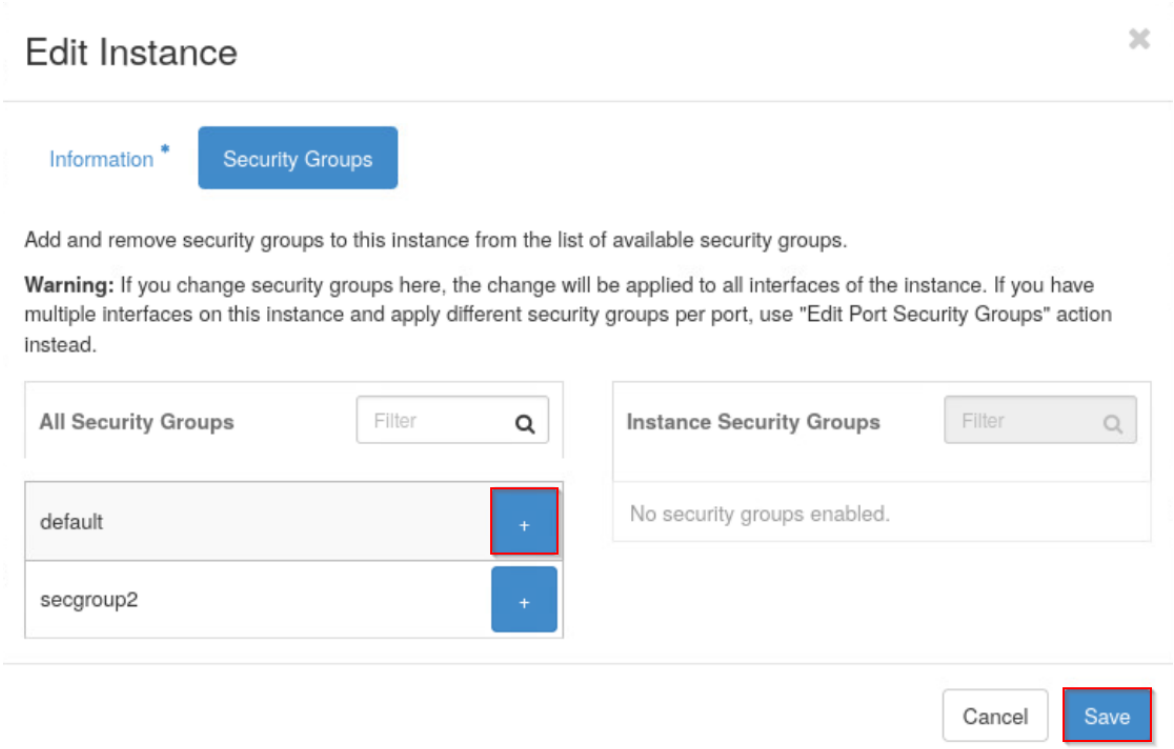
Note

This option will edit security groups for all interfaces on the instance. Notice that there is also an option to **Edit Port Security Groups**, which allows you to edit security groups for individual interfaces on the instance.

6.19. In the **Edit Instance** popup, the **Instance Security Groups** list contains the security groups that are currently applied to the instance. Remove **secgroup2** from this instance by clicking the - button next to that group, and click **Save** to finalize the change.



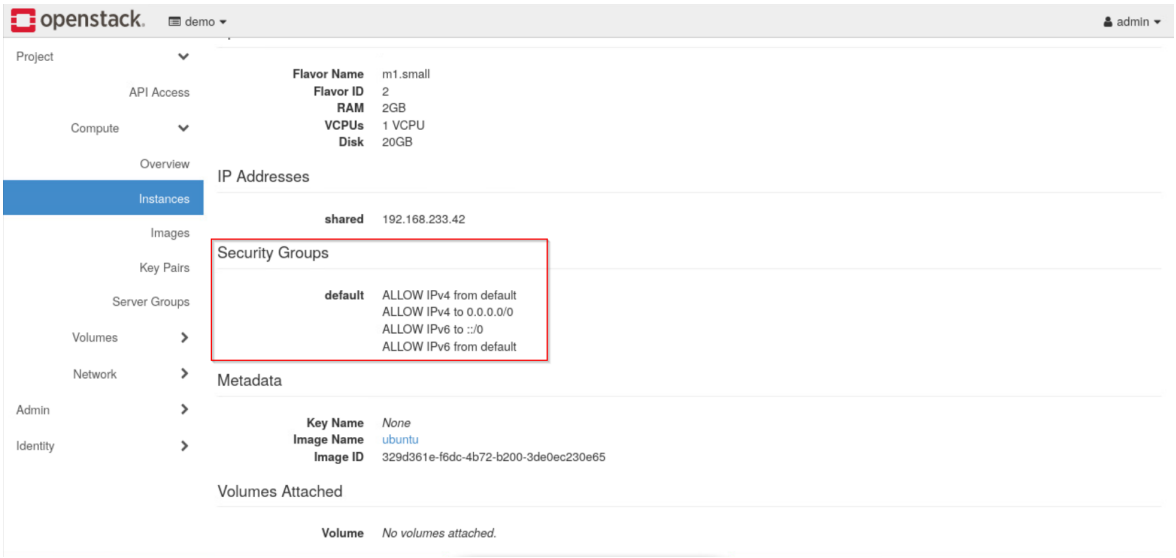
6.20. Re-open the popup by clicking the dropdown next to **Create Snapshot** and clicking **Edit Security Groups**. The **All Security Groups** list contains the security groups that are available but are not currently applied to the instance. Add the **default** security group to the interface by clicking the + button next to that group, and click **Update** to finalize the change.



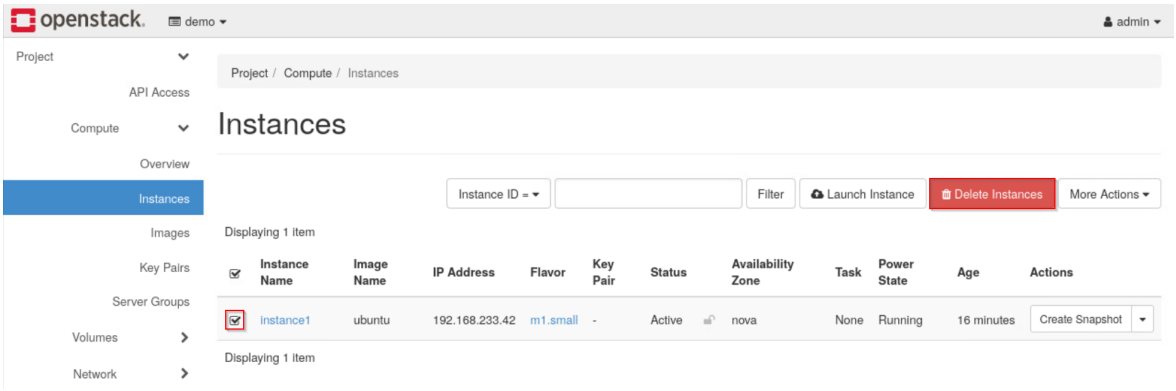
Tip

You can assign and unassign multiple security groups before saving the changes.

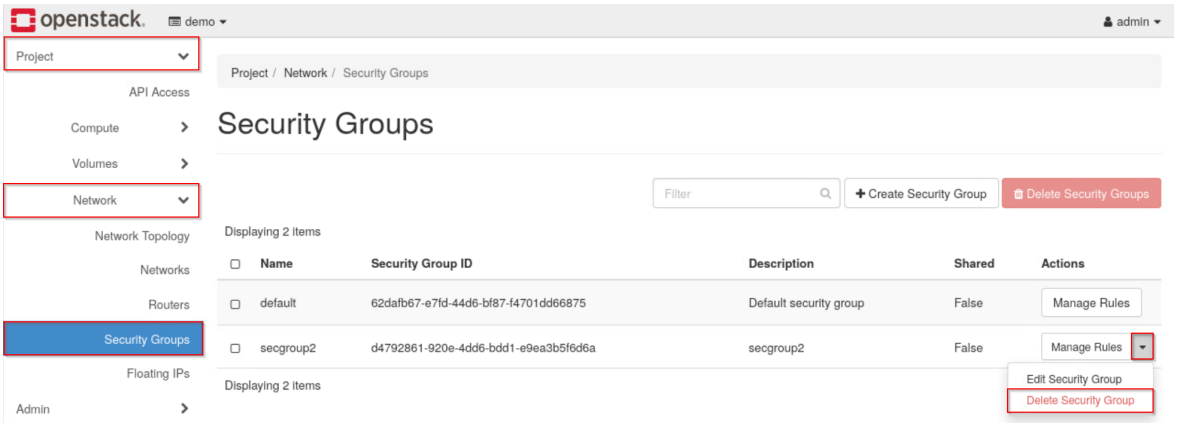
6.21. To verify that the security group has been applied again, click **instance1**. On the *Overview* tab of the *instance1* page, scroll down to view the *Security Groups* section. This time, you should see the **default** security group and its rules listed.



6.22. We no longer need this instance, so navigate back to **Project** > **Compute** > **Instances**, select **instance1**, and click **Delete Instances**.



6.23. We will also recreate the security group in the final section of the lab in order to show a complete example, so we can safely delete **secgroup2**. To delete the security group from the dashboard, navigate to **Project** > **Network** > **Security Groups**. Click the dropdown next to the **Manage Rules** button in the same row as **secgroup2**, and then click **Delete Security Group**.



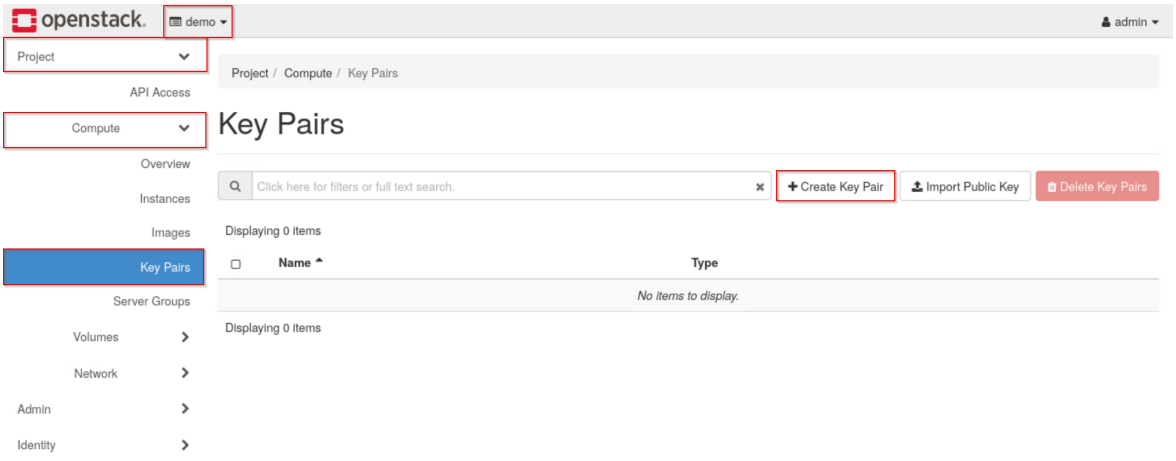
6.24. Leave the web browser open, and continue to the next task.

7 Creating SSH Key Pairs

In this task, you will use the *Horizon Dashboard* and *OpenStack Unified CLI* to create and manage SSH key pairs. These keys will later be used to securely connect to external instances from outside the OpenStack environment.

7.1. If the web browser is not already open, open it. Navigate to **192.168.1.20**, and log in to the dashboard as **admin** with the password **secret**.

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



7.3. 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

When creating key pairs from the Horizon Dashboard, the private key file permissions are *not* set strictly, so it is recommended to still set them through the command line. We will do this in the following steps.

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

7.5. 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)]:~$
```

7.6. 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/keypair1.pem
```

```
[ubuntu@workstation (keystone-admin)]:~$ chmod 600 ~/Downloads/keypair1.pem
[ubuntu@workstation (keystone-admin)]:~$
```

7.7. 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.

7.8. 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)]:~$
```

7.9. List the available key pairs to verify that **keypair1** was deleted.

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

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

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

7.10. 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)]:~$
```

7.11. Set the file permissions of the private key so that only the **ubuntu** user has read/write permissions.

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

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

7.12. List the available key pairs to verify the creation of **keypair2**.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack keypair list
+----------+-------------------------------------------------+
| Name     | Fingerprint                                     |
+----------+-------------------------------------------------+
| keypair2 | 6f:46:7c:56:38:82:f3:d2:f6:97:b1:65:ae:c0:90:87 |
+----------+-------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

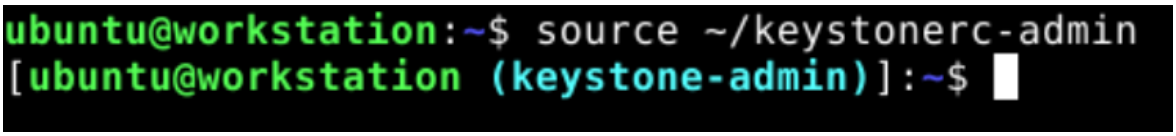
7.13. Leave the terminal window open and continue to the next task.

8 Applying SSH Keys to Instances

In this task, you will use both the *Horizon Dashboard* and *OpenStack Unified CLI* to apply SSH key pairs to instances. This is the final piece necessary to have an instance that can be reached and logged in to from an external network, which the next task will explore.

8.1. 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
```



8.2. An SSH key can be applied to an instance at creation from the command line. Create an instance with the **keypair2** key pair.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --network shared \
> --key-name keypair2 \
> instance1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --network shared \
> --key-name keypair2 \
> 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                           | XTL7K7hqoZwi                         |
| config_drive                        |                                      |
| created                             | 2025-06-30T15:52:26Z                 |
| flavor                              | m1.small (2)                         |
| hostId                              |                                      |
| id                                  | a498cf56-8910-4525-b446-a48141b6b7b7 |
| image                               | ubuntu (329d361e-f6dc-               |
|                                     | 4b72-b200-3de0ec230e65)              |
| key_name                            | keypair2                             |
| name                                | instance1                            |
| progress                            | 0                                    |
| project_id                          | 39e851b14f864573aad60582c35e40dc     |
| properties                          |                                      |
| security_groups                     | name='default'                       |
| status                              | BUILD                                |
| updated                             | 2025-06-30T15:52:26Z                 |
| user_id                             | 14f5376f00c04e90b7103dd8d4263040     |
| volumes_attached                    |                                      |
+-------------------------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

OpenStack does not provide a way to directly change the key pair associated with an existing instance. We will not need to in these labs, but if you need to use a different SSH key, one option is to manually add your new key to the **/.ssh/authorized_keys** file inside the instance. However, this change will not be tracked by OpenStack. Another option is to rebuild the instance with a new key pair. If the instance contains important data, it's important to back it up—for example, with a snapshot (covered later).

8.3. Verify that **keypair2** is attached to **instance1**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server show \
> -c key_name \
> instance1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server show \
> -c key_name \
> instance1
+----------+----------+
| Field    | Value    |
+----------+----------+
| key_name | keypair2 |
+----------+----------+
[ubuntu@workstation (keystone-admin)]:~$
```

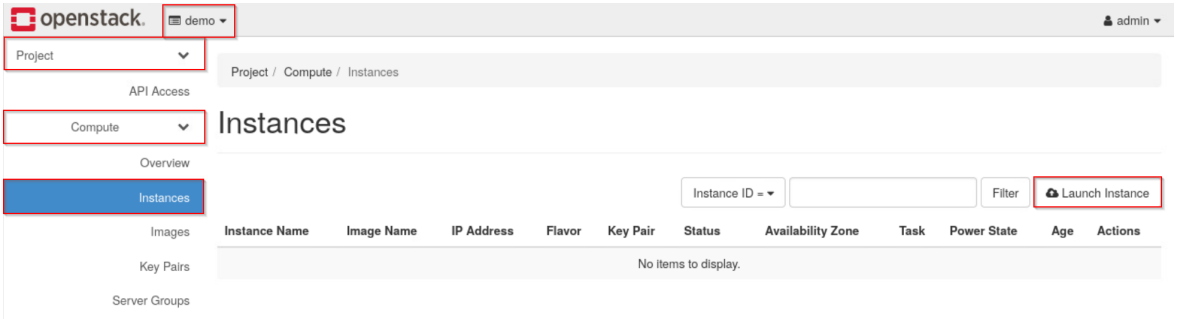
8.4. Delete **instance1**. We will recreate it from the Horizon Dashboard to demonstrate adding a security group to an instance at creation time from the dashboard.

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

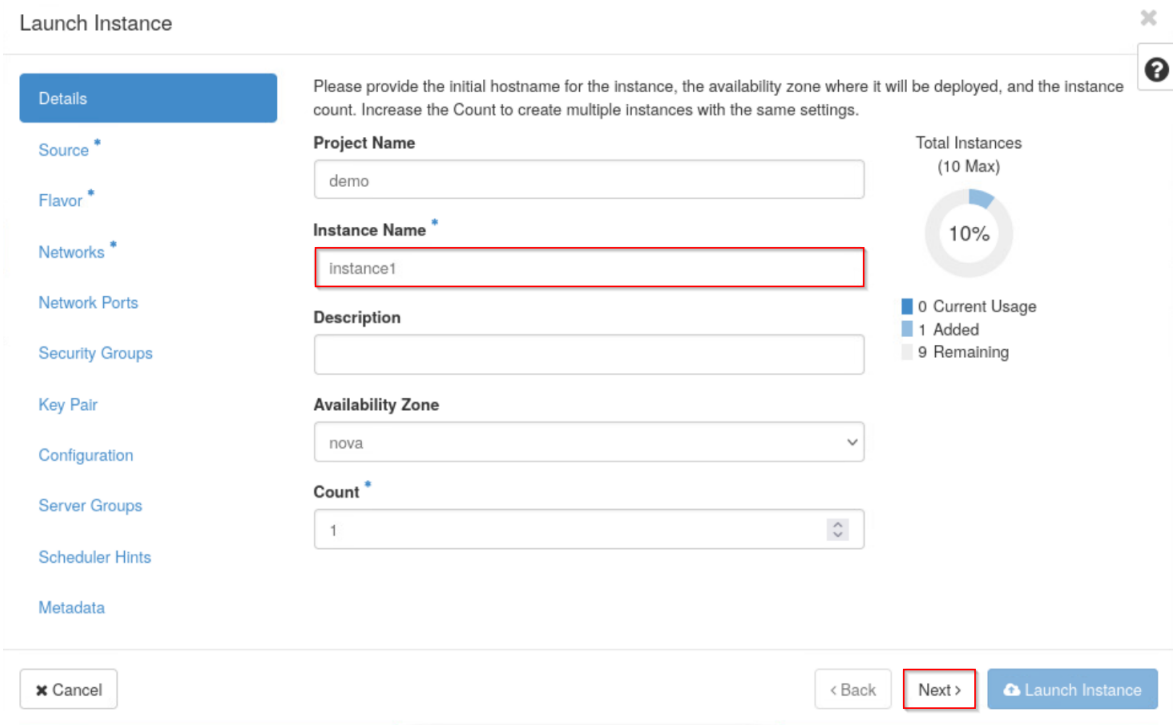
```
[ubuntu@workstation (keystone-admin)]:~$ openstack server delete instance1
[ubuntu@workstation (keystone-admin)]:~$
```

8.5. Leave the terminal window open, and open the web browser. Navigate to **192.168.1.20**, and log in to the dashboard as **admin** with the password **secret**.

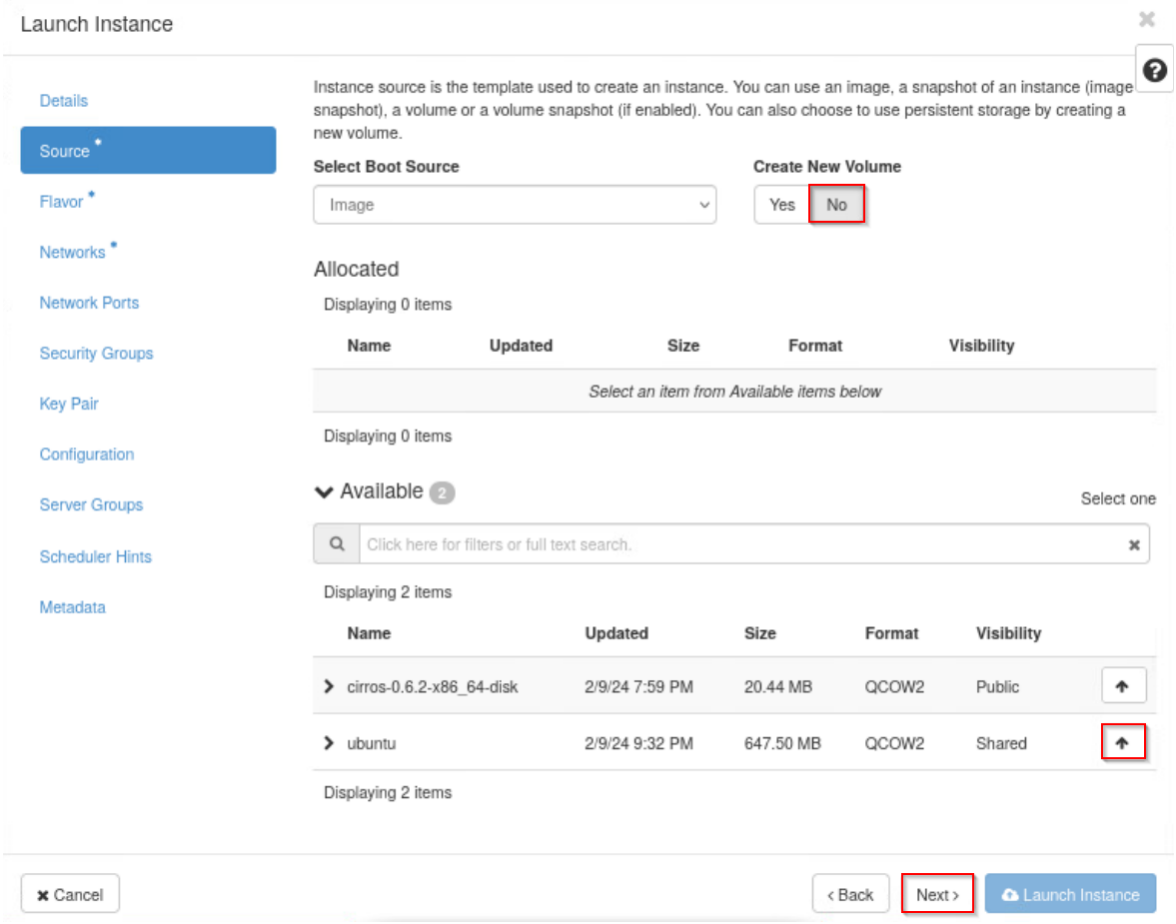
8.6. Select the **demo** project. Navigate to **Project** > **Compute** > **Instances**, and click **Launch Instance**.



8.7. In the *Details* tab, type **instance1** in the *Instance Name* field. Click **Next**.



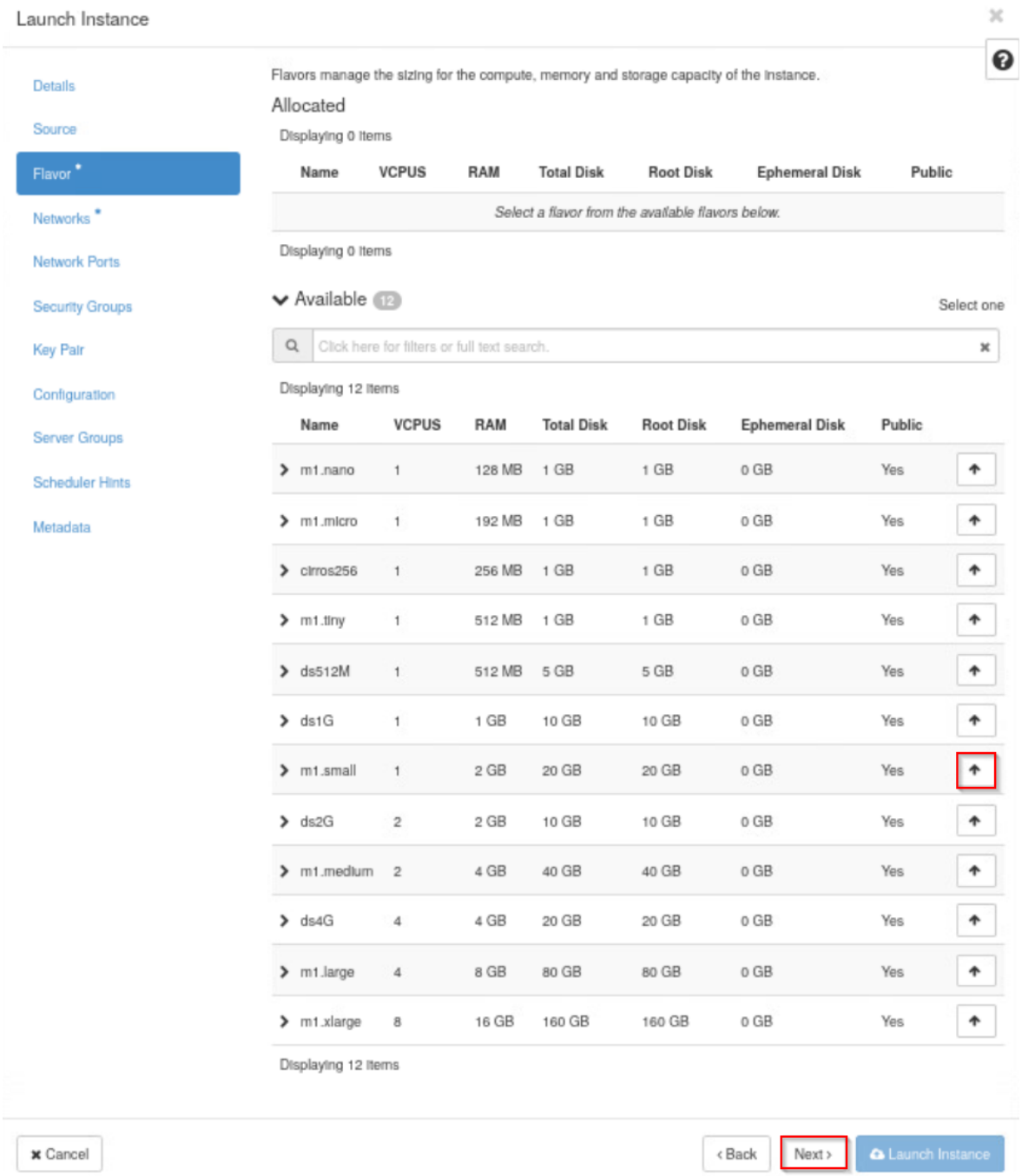
8.8. In the *Source* tab, set *Create New Volume* to **No**, and scroll down (if needed) to select the **ubuntu** image. Click **Next**.



Stop

Before proceeding to the next step, confirm that **ubuntu** appears in the *Allocated* section.

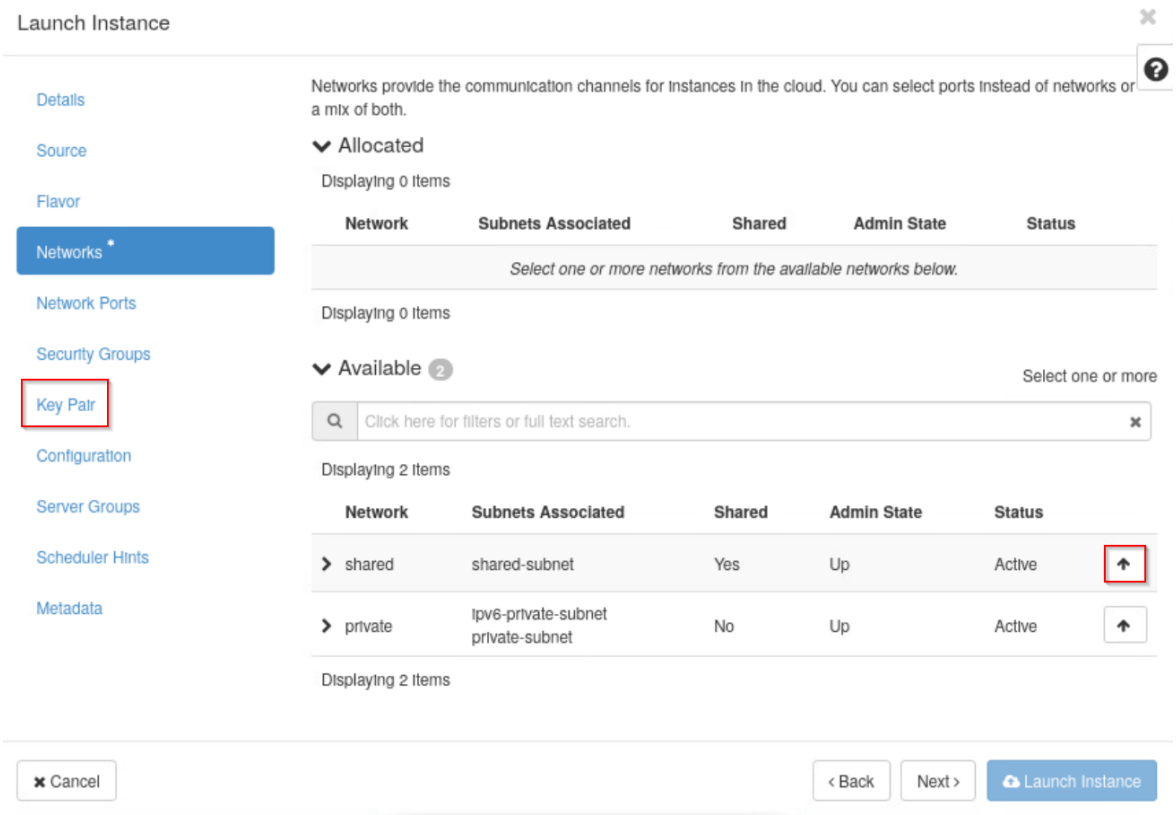
8.9. In the *Flavor* tab, scroll down (if needed) to select the **m1.small** flavor. Click **Next**.



Stop

Before proceeding to the next step, confirm that **m1.small** appears in the *Allocated* section.

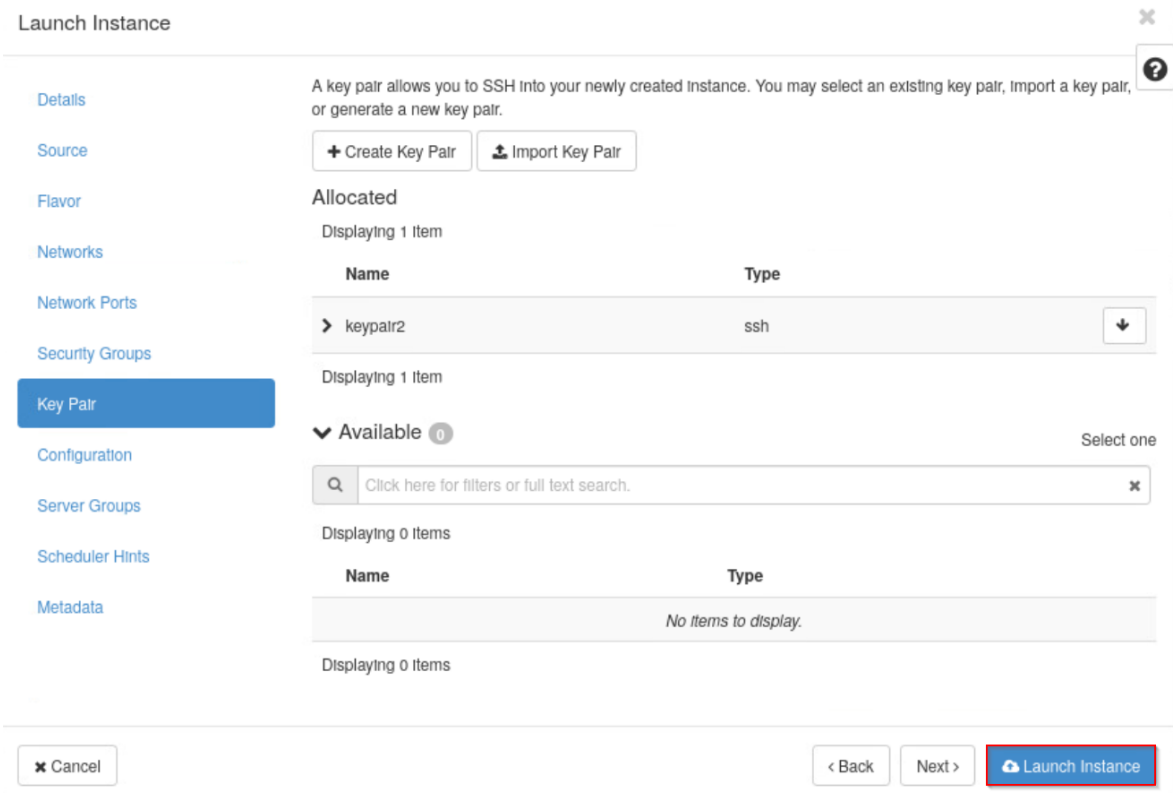
8.10. In the *Networks* tab, select the **shared** network. Navigate to the *Key Pair* tab.



Stop

Before proceeding to the next step, confirm that **shared** appears in the *Allocated* section.

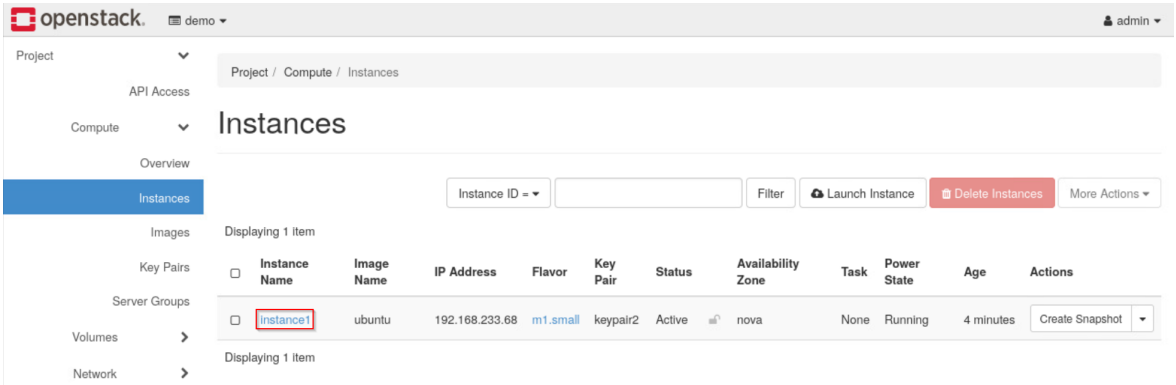
8.11. In the *Key Pair* tab, select **keypair2** if it is not already in the *Allocated* section, and click **Launch Instance**.



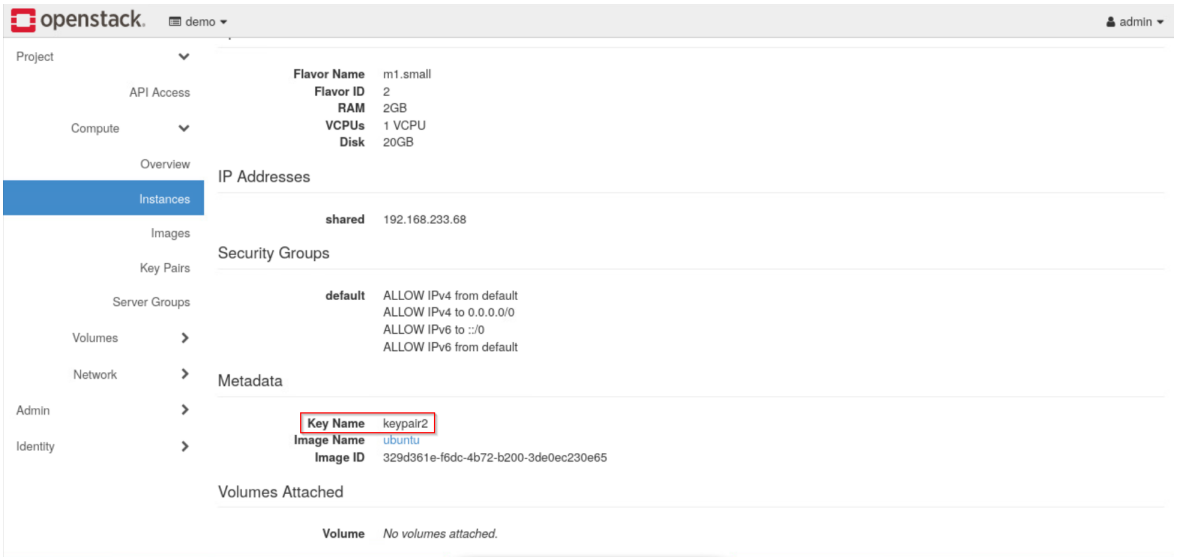
Stop

Before proceeding to the next step, confirm that **keypair2** appears in the *Allocated* section.

8.12. You should be redirected to the **Project** > **Compute** > **Instances** page. To verify that the key pair was applied, first click **instance1** to go to the instance's details page.



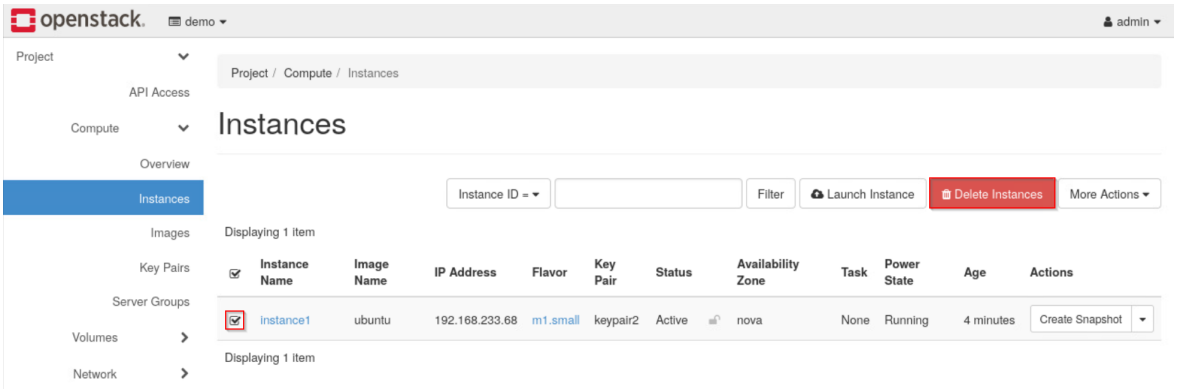
8.13. Scroll down to the *Metadata* section and verify that **keypair2** is present in the *Key Name* row.



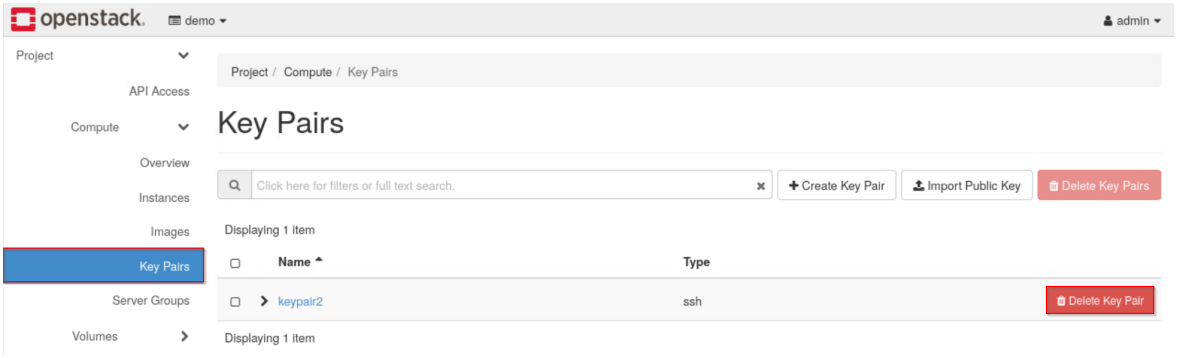
Note

If an instance does not have a key pair, the *Key Name* row will show "None".

8.14. We no longer need this instance, so navigate back to **Project** > **Compute** > **Instances**, select **instance1**, and click **Delete Instances**.



8.15. We will also recreate the key pair in the final section of the lab in order to show a complete example. So, we can safely delete **keypair2**. To delete the key pair from the dashboard, navigate to **Project** > **Compute** > **Key Pairs**, and click the **Delete Key Pair** button in the same row as **keypair2**.



8.16. Log out of the *Horizon Dashboard*, and close the web browser. Continue to the next task.

9 Launching and Verifying an External Instance

Up to this point, we have learned how to create 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 put all these concepts together to create a functioning external instance. You will create the necessary resources, launch an external instance, and verify its connectivity and functionality with the **ssh** and **ping** commands.

9.1. 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
```

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

9.2. Before creating our own router and external network, we need to delete the ones that are created by default. First, unset the external gateway from **router1**.

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

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

9.3. List the interfaces of **router1**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack port list \
> -c ID \
> -f value \
> --router router1
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack port list \
> -c ID \
> -f value \
> --router router1
a05f4e1c-4014-4d25-9538-64e8114197e1
d369b706-db4a-4239-b715-721708931870
[ubuntu@workstation (keystone-admin)]:~$
```

9.4. Capture the output of the previous command in to a variable called **ports**.

```
[ubuntu@workstation (keystone-admin)]:~$ ports=$(!!)
```

```
[ubuntu@workstation (keystone-admin)]:~$ ports=$(!!)
ports=$(openstack port list -c ID -f value --router router1)
[ubuntu@workstation (keystone-admin)]:~$
```

9.5. Ensure that **ports** contains the ID values as expected.

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

```
[ubuntu@workstation (keystone-admin)]:~$ echo $ports
a05f4e1c-4014-4d25-9538-64e8114197e1 d369b706-db4a-4239-b715-721708931870
[ubuntu@workstation (keystone-admin)]:~$
```

9.6. Remove the interfaces from **router1**.

```
[ubuntu@workstation (keystone-admin)]:~$ for port in $ports; do \
> openstack router remove port router1 $port; \
> done
```

```
[ubuntu@workstation (keystone-admin)]:~$ for port in $ports; do \
> openstack router remove port router1 $port; \
> done
[ubuntu@workstation (keystone-admin)]:~$
```

9.7. Delete **router1**.

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

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

9.8. Delete the **public** network.

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

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

9.9. First, we will create an external network. List the existing networks to ensure that one does not already exist. Only the **shared** and **private** networks should be listed in the output.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list
+--------------------------------------+---------+--------------------------------------+
| ID                                   | Name    | Subnets                              |
+--------------------------------------+---------+--------------------------------------+
| 966ecb4f-                            | private | 674205b6-1357-4727-a21a-             |
| 4ff8-44ea-a476-2d2f18955085          |         | 94220492a57f, fa8a2545-5a8c-44a2     |
|                                      |         | -bacc-1b86c253b880                   |
| 9f23266f-d833-4337-9a27-4818a6d      | shared  | 7e456257-76e5-4cfc-bf3f-             |
| 28e9e                                |         | b2a3876dba40                         |
+--------------------------------------+---------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.10. Create an external network named **external**. 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 \
> external
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network create \
> --external \
> --share \
> --provider-network-type flat \
> --provider-physical-network public \
> external
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | UP                                   |
| availability_zone_hints   |                                      |
| availability_zones        |                                      |
| created_at                | 2025-07-02T15:57:18Z                 |
| description               |                                      |
| dns_domain                | None                                 |
| id                        | c231ef7c-399a-41ee-b95a-911d9a2abdbe |
| ipv4_address_scope        | None                                 |
| ipv6_address_scope        | None                                 |
| is_default                | False                                |
| is_vlan_transparent       | None                                 |
| mtu                       | 1500                                 |
| name                      | external                             |
| 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                | 2025-07-02T15:57:18Z                 |
+---------------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.11. Create a subnet named **external-subnet** in the **external** 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 and 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 external \
> external-subnet
```

```
[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 external \
> external-subnet
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| allocation_pools  | 172.25.250.60-172.25.250.80          |
| cidr              | 172.25.250.0/24                      |
| created_at        | 2025-07-02T15:58:58Z                 |
| description       |                                      |
| dns_nameservers   | 172.25.250.254                       |
| enable_dhcp       | False                                |
| gateway_ip        | 172.25.250.254                       |
| host_routes       |                                      |
| id                | 1e2fe0a9-5ed4-4e00-aeb5-6040164f6bdf |
| ip_version        | 4                                    |
| ipv6_address_mode | None                                 |
| ipv6_ra_mode      | None                                 |
| name              | external-subnet                      |
| network_id        | c231ef7c-399a-41ee-b95a-911d9a2abdbe |
| project_id        | 39e851b14f864573aad60582c35e40dc     |
| revision_number   | 0                                    |
| segment_id        | None                                 |
| service_types     |                                      |
| subnetpool_id     | None                                 |
| tags              |                                      |
| updated_at        | 2025-07-02T15:58:58Z                 |
+-------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.12. List the networks again to verify the creation of the **external** network.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack network list
+--------------------------------------+----------+--------------------------------------+
| ID                                   | Name     | Subnets                              |
+--------------------------------------+----------+--------------------------------------+
| 966ecb4f-                            | private  | 674205b6-1357-4727-a21a-             |
| 4ff8-44ea-a476-2d2f18955085          |          | 94220492a57f, fa8a2545-5a8c-         |
|                                      |          | 44a2-bacc-1b86c253b880               |
| 9f23266f-d833-4337-9a27-4818a6d      | shared   | 7e456257-76e5-4cfc-bf3f-             |
| 28e9e                                |          | b2a3876dba40                         |
| c231ef7c-399a-41ee-b95a-             | external | 1e2fe0a9-5ed4-4e00-aeb5-6040164      |
| 911d9a2abdbe                         |          | f6bdf                                |
+--------------------------------------+----------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.13. List the existing routers. The output should be empty.

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

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

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

9.14. Next, create a router named **router-external**.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router create router-external
+-------------------------+--------------------------------------+
| Field                   | Value                                |
+-------------------------+--------------------------------------+
| admin_state_up          | UP                                   |
| availability_zone_hints |                                      |
| availability_zones      |                                      |
| created_at              | 2025-07-02T16:00:14Z                 |
| description             |                                      |
| distributed             | False                                |
| external_gateway_info   | None                                 |
| flavor_id               | None                                 |
| ha                      | False                                |
| id                      | f6d6293d-86cf-4c7b-bab4-07cca9757d2e |
| name                    | router-external                      |
| project_id              | 39e851b14f864573aad60582c35e40dc     |
| revision_number         | 1                                    |
| routes                  |                                      |
| status                  | ACTIVE                               |
| tags                    |                                      |
| updated_at              | 2025-07-02T16:00:14Z                 |
+-------------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.15. List the routers again to verify the creation of **router-external**.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router list
+--------------------------------------+-----------------+--------+-------+-------------+-------+----------------------------------+
| ID                                   | Name            | Status | State | Distributed | HA    | Project                          |
+--------------------------------------+-----------------+--------+-------+-------------+-------+----------------------------------+
| f6d6293d-86cf-4c7b-bab4-07cca9757d2e | router-external | ACTIVE | UP    | False       | False | 39e851b14f864573aad60582c35e40dc |
+--------------------------------------+-----------------+--------+-------+-------------+-------+----------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.16. The router needs to be connected to both the **shared-subnet** and **external-subnet** networks to allow external connections to the instance. First, add the **shared-subnet** to the router.

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

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

9.17. Set the **external** network as the gateway for the router.

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

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

9.18. Show the details of **router-external** to show that it is connected to two subnets.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack router show router-external
+-------------------------+-----------------------------------------------------+
| Field                   | Value                                               |
+-------------------------+-----------------------------------------------------+
| admin_state_up          | UP                                                  |
| availability_zone_hints |                                                     |
| availability_zones      |                                                     |
| created_at              | 2025-07-02T16:00:14Z                                |
| description             |                                                     |
| distributed             | False                                               |
| external_gateway_info   | {"network_id": "c231ef7c-399a-41ee-b95a-            |
|                         | 911d9a2abdbe", "enable_snat": true,                 |
|                         | "external_fixed_ips": [{"subnet_id":                |
|                         | "1e2fe0a9-5ed4-4e00-aeb5-6040164f6bdf",             |
|                         | "ip_address": "172.25.250.76"}]}                    |
| flavor_id               | None                                                |
| ha                      | False                                               |
| id                      | f6d6293d-86cf-4c7b-bab4-07cca9757d2e                |
| interfaces_info         | [{"subnet_id": "7e456257-76e5-4cfc-bf3f-            |
|                         | b2a3876dba40", "ip_address": "192.168.233.1",       |
|                         | "port_id": "9288a863-28c3-421a-9a5e-7346d30ea66c"}] |
| name                    | router-external                                     |
| project_id              | 39e851b14f864573aad60582c35e40dc                    |
| revision_number         | 4                                                   |
| routes                  |                                                     |
| status                  | ACTIVE                                              |
| tags                    |                                                     |
| updated_at              | 2025-07-02T16:01:46Z                                |
+-------------------------+-----------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.19. Now, we will create a floating IP address to associate with the instance. This will be the IP address we use to connect to the instance through the **external** network. First, list the available floating IP addresses. The output should be empty.

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

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

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

9.20. Create the floating IP address **172.25.250.75** in the **external** network.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip create \
> --floating-ip-address 172.25.250.75 \
> external
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| created_at          | 2025-07-02T16:03:11Z                 |
| description         |                                      |
| fixed_ip_address    | None                                 |
| floating_ip_address | 172.25.250.75                        |
| floating_network_id | c231ef7c-399a-41ee-b95a-911d9a2abdbe |
| id                  | 845f62f4-c0bc-4ba4-989c-f42bf60ed3cc |
| 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          | 2025-07-02T16:03:11Z                 |
+---------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.21. List the floating IP addresses again to verify the creation of **172.25.250.75**.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip list
+------------+---------------------+------------------+------+------------------+---------------+
| ID         | Floating IP Address | Fixed IP Address | Port | Floating Network | Project       |
+------------+---------------------+------------------+------+------------------+---------------+
| 845f62f4   | 172.25.250.75       | None             | None | c231ef7c-399a-   | 39e851b14f8645 |
| -c0bc-4ba4 |                     |                  |      | 41ee-b95a-       | 73aad60582c35e |
| -989c-f42bf |                     |                  |      | 911d9a2abdbe     | 40dc           |
| 60ed3cc    |                     |                  |      |                  |               |
+------------+---------------------+------------------+------+------------------+---------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.22. In order for our ICMP and SSH requests to reach our external instance, we need to set up a security group and security rules that allow this traffic. First, list the available security groups. The output should contain two default security groups.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group list
+----------------------+---------+----------------------+----------------------+
| ID                   | Name    | Description          | Project              |
+----------------------+---------+----------------------+----------------------+
| 2f0f5133-8396-45ea-  | default | Default security     | eb2dcd08d8ae46ffac3f1 |
| a4de-61945d79ed2e    |         | group                | 6c3973ef61d          |
| 62dafb67-e7fd-44d6-b | default | Default security     | 39e851b14f864573aad60 |
| f87-f4701dd66875     |         | group                | 582c35e40dc          |
+----------------------+---------+----------------------+----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.23. Create a security group. Because we will allow ICMP and SSH traffic, we will name the security group **sg-allow-icmp-ssh**.

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group create \
> sg-allow-icmp-ssh
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group create \
> sg-allow-icmp-ssh
+-----------------+-------------------------------------------------------------+
| Field           | Value                                                       |
+-----------------+-------------------------------------------------------------+
| created_at      | 2025-07-02T16:09:59Z                                        |
| description     | sg-allow-icmp-ssh                                           |
| id              | ed0d9549-6476-4a35-a2d1-24f140db7c73                        |
| name            | sg-allow-icmp-ssh                                           |
| project_id      | 39e851b14f864573aad60582c35e40dc                            |
| revision_number | 1                                                           |
| rules           | created_at='2025-07-02T16:09:59Z', direction='egress',      |
|                 | ethertype='IPv4', id='0b2244a9-b588-40e4-aeaa-              |
|                 | 1ee04281d927', standard_attr_id='54',                       |
|                 | updated_at='2025-07-02T16:09:59Z'                           |
|                 | created_at='2025-07-02T16:09:59Z', direction='egress',      |
|                 | ethertype='IPv6',                                           |
|                 | id='f925dbf8-9bc9-48b5-92f2-64106c8f34f5',                  |
|                 | standard_attr_id='53', updated_at='2025-07-02T16:09:59Z'    |
| updated_at      | 2025-07-02T16:09:59Z                                        |
+-----------------+-------------------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

Real-world OpenStack environments may have a variety of instances with different security group needs. Therefore, it pays to be descriptive in your naming conventions so that you can more easily identify the appropriate security group later. It is much easier to tell what **sg-allow-icmp-ssh** does than it is to guess the purpose of **secgroup1**. However, giving strong names alone is not enough—it is always best to check a security group's actual rules before adding it to an instance.

9.24. List the security groups to verify the creation of **sg-allow-icmp-ssh**.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group list
+--------------------+--------------------+--------------------+--------------------+
| ID                 | Name               | Description        | Project            |
+--------------------+--------------------+--------------------+--------------------+
| 2f0f5133-8396      | default            | Default security   | eb2dcd08d8ae46ffa  |
| -45ea-a4de-        |                    | group              | c3f16c3973ef61d    |
| 61945d79ed2e       |                    |                    |                    |
| 62dafb67-e7fd-44d  | default            | Default security   | 39e851b14f864573a  |
| 6-bf87-f4701dd668  |                    | group              | ad60582c35e40dc    |
| 75                 |                    |                    |                    |
| ed0d9549-6476-4a3  | sg-allow-icmp-ssh  | sg-allow-icmp-ssh  | 39e851b14f864573a  |
| 5-a2d1-24f140db7c  |                    |                    | ad60582c35e40dc    |
| 73                 |                    |                    |                    |
+--------------------+--------------------+--------------------+--------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.25. List the rules in the **sg-allow-icmp-ssh** security group. There should be two rules created by default.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> sg-allow-icmp-ssh
+--------------------+-------------+----------+------------+-----------------------+
| ID                 | IP Protocol | IP Range | Port Range | Remote Security Group |
+--------------------+-------------+----------+------------+-----------------------+
| 0b2244a9-b588-40e4 | None        | None     |            | None                  |
| -aeaa-1ee04281d927 |             |          |            |                       |
| f925dbf8-9bc9-48b5 | None        | None     |            | None                  |
| -92f2-64106c8f34f5 |             |          |            |                       |
+--------------------+-------------+----------+------------+-----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

Tip

Try to use the **for** loop trick to verify that the default security rules allow IPv4 and IPv6 egress traffic. You can use this command to show the details of a rule:

```
openstack security group rule show <ID>
```

9.26. Add a security rule in the **sg-allow-icmp-ssh** security group to allow all incoming ICMP traffic.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule create \
> --protocol icmp \
> sg-allow-icmp-ssh
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| created_at        | 2025-07-02T16:11:55Z                 |
| description       |                                      |
| direction         | ingress                              |
| ether_type        | IPv4                                 |
| id                | deefbca4-8ba4-4ee8-9131-6b8e8d2903b7 |
| 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 | ed0d9549-6476-4a35-a2d1-24f140db7c73 |
| updated_at        | 2025-07-02T16:11:55Z                 |
+-------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.27. 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 \
> sg-allow-icmp-ssh
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule create \
> --protocol tcp \
> --dst-port 22 \
> sg-allow-icmp-ssh
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| created_at        | 2025-07-02T16:12:48Z                 |
| description       |                                      |
| direction         | ingress                              |
| ether_type        | IPv4                                 |
| id                | 6df08e02-9958-4e04-9603-e4ce8caa3f49 |
| 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 | ed0d9549-6476-4a35-a2d1-24f140db7c73 |
| updated_at        | 2025-07-02T16:12:48Z                 |
+-------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.28. List the rules of the **sg-allow-icmp-ssh** security group again to verify that there are now four rules: the two default rules plus the two rules you just added.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack security group rule list \
> sg-allow-icmp-ssh
+--------------------+-------------+-----------+------------+-----------------------+
| ID                 | IP Protocol | IP Range  | Port Range | Remote Security Group |
+--------------------+-------------+-----------+------------+-----------------------+
| 0b2244a9-b588-40e  | None        | None      |            | None                  |
| 4-aeaa-            |             |           |            |                       |
| 1ee04281d927       |             |           |            |                       |
| 6df08e02-9958-4e0  | tcp         | 0.0.0.0/0 | 22:22      | None                  |
| 4-9603-e4ce8caa3f  |             |           |            |                       |
| 49                 |             |           |            |                       |
| deefbca4-8ba4-4ee  | icmp        | 0.0.0.0/0 |            | None                  |
| 8-9131-6b8e8d2903  |             |           |            |                       |
| b7                 |             |           |            |                       |
| f925dbf8-9bc9-48b  | None        | None      |            | None                  |
| 5-92f2-64106c8f34  |             |           |            |                       |
| f5                 |             |           |            |                       |
+--------------------+-------------+-----------+------------+-----------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.29. Finally, we need an SSH key pair to remotely log in to the external instance. List the available key pairs. The output should be empty.

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

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

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

9.30. Create a key pair called **keypair**, and save the private key to **/Downloads/keypair.pem**.

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

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

9.31. Set the file permissions of the private key so that only the **ubuntu** user has read/write permissions.

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

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

9.32. List the available key pairs again to verify the creation of **keypair**.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack keypair list
+---------+-------------------------------------------------+
| Name    | Fingerprint                                     |
+---------+-------------------------------------------------+
| keypair | 66:30:11:e1:98:80:8c:47:d2:a9:f0:c9:62:5e:4a:33 |
+---------+-------------------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.33. We now have all the resources we need to create an external instance. List all instances in the project. The output should be empty.

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

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

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

9.34. 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 \
> --network shared \
> --security-group sg-allow-icmp-ssh \
> --key-name keypair \
> instance-external
```

```
[ubuntu@workstation (keystone-admin)]:~$ openstack server create \
> --image ubuntu \
> --flavor m1.small \
> --network shared \
> --security-group sg-allow-icmp-ssh \
> --key-name keypair \
> instance-external
+-------------------------------------+--------------------------------------+
| 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                           | DM33HA3CWcci                         |
| config_drive                        |                                      |
| created                             | 2025-07-02T16:16:30Z                 |
| flavor                              | m1.small (2)                         |
| hostId                              |                                      |
| id                                  | 174dbcb2-0d5f-4f19-b6f2-729d8dbaa540 |
| image                               | ubuntu (329d361e-f6dc-               |
|                                     | 4b72-b200-3de0ec230e65)              |
| key_name                            | keypair                              |
| name                                | instance-external                    |
| progress                            | 0                                    |
| project_id                          | 39e851b14f864573aad60582c35e40dc     |
| properties                          |                                      |
| security_groups                     | name='ed0d9549-6476-4a35-a2d1-24f140db7 |
|                                     | c73'                                 |
| status                              | BUILD                                |
| updated                             | 2025-07-02T16:16:29Z                 |
| user_id                             | 14f5376f00c04e90b7103dd8d4263040     |
| volumes_attached                    |                                      |
+-------------------------------------+--------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.35. List the floating IPs.

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

```
[ubuntu@workstation (keystone-admin)]:~$ openstack floating ip list
+------------+--------------------+------------------+------+------------------+---------------+
| ID         | Floating IP Address | Fixed IP Address | Port | Floating Network | Project       |
+------------+--------------------+------------------+------+------------------+---------------+
| 845f62f4   | 172.25.250.75      | None             | None | c231ef7c-399a-   | 39e851b14f8645 |
| -c0bc-4ba4 |                    |                  |      | 41ee-b95a-       | 73aad60582c35e |
| -989c-f42bf |                   |                  |      | 911d9a2abdbe     | 40dc          |
| 60ed3cc    |                    |                  |      |                  |               |
+------------+--------------------+------------------+------+------------------+---------------+
[ubuntu@workstation (keystone-admin)]:~$
```

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

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

9.37. 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=192.168.233.230, 172.25.250.75 |
+-------------------+----------------------------------------+
[ubuntu@workstation (keystone-admin)]:~$
```

9.38. 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/keypair.pem \
> 192.168.1.20:~/keypair.pem
```

```
[ubuntu@workstation (keystone-admin)]:~$ scp ~/Downloads/keypair.pem \
> 192.168.1.20:~/keypair.pem
ubuntu@192.168.1.20's password:
keypair.pem                                   100% 1680     2.9MB/s   00:00
[ubuntu@workstation (keystone-admin)]:~$
```

> **Note**
>
> Because your username is **ubuntu** on both machines, you don't need to specify the username in the **scp** command. By default, **scp** uses your current local username for the remote connection. If you wanted to send the file to a different user, such as **user2** on the **devstack** machine, you would write: **user2@192.168.1.20:~/keypair.pem**.

9.39. 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 I
nternet connection or proxy settings

Last login: Thu Oct 17 01:27:44 2024
ubuntu@devstack:~$
```

9.40. Ping the **instance-external** instance with the floating IP that was assigned to it in the previous task. This will verify that the instance can be reached and that its security group allows ICMP ingress traffic.

```
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.

9.41. 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 ~/keypair.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:u75EWhnyJ8tc8P2xb3bIrBITODw+9uEhXahNpjuG8/o.
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 Wed Jul  2 16:27:20 UTC 2025

  System load:  0.2216796875      Processes:             85
  Usage of /:   7.4% of 19.20GB   Users logged in:       0
  Memory usage: 8%                IPv4 address for ens3: 192.168.233.230
  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.

9.42. 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.

9.43. The lab is now complete.

A Fine-Grained Security Group Control

In Section 6, we discussed applying security groups to instances. However, in reality, security groups are applied to the individual ports on an instance. For simplicity, we could mostly ignore this distinction and treat them as if they applied directly to the instance. More fine-grained control over security groups is available from both the CLI and web interface, which is especially useful when working with instances that have multiple interfaces that each have different requirements.

From the dashboard, managing security groups for individual ports only requires navigating a new menu. In Section 6, Step 18, we clicked **Edit Security Groups** in the instance's dropdown menu. To manage security groups for a specific interface instead, click **Edit Port Security Groups**. The interface is nearly identical.

From the CLI, working with individual ports requires slightly different commands. The following commands apply to the *entire* instance—that is, to all its ports (with some exceptions):

```
openstack server add security group <instance> <security_group>
openstack server remove security group <instance> <security_group>
```

Security groups can also be managed for each port from the CLI; however, the process can be slightly more cumbersome because unnamed ports must be specified by ID.

First, it is recommended to maximize your terminal window to prevent ID values from being split across lines. This will make it easier to copy the IDs to the clipboard. View the ports of an instance to get their IDs.

```
openstack port list --server <instance_name_or_id>
```

For each port you want to modify, first copy its ID to the clipboard. Alternatively, use the ID to name the port with

```
openstack port set --name <new_port_name> <port_name_or_id>
```

or name a port upon creation with

```
openstack port create --name <port_name> --network <network_name_or_id>
```

Next, find the security groups applied to the port.

```
openstack port show <port_name_or_id> -c security_group_ids
```

Optionally, find the name of each security group.

```
openstack security group show <security_group_id> -c name
```

Finally, remove a security group from an interface individually with

```
openstack port unset --security-group <security_group_name_or_id> <port_name_or_id>
```

or remove all security groups from an interface with

```
openstack port set --no-security-group <port_name_or_id>
```