Preventing East-West Attacks Across Tenant Projects in OpenStack

LAB #4

Bryan Daniel, Justin, Cockrell, and Dylan Hagy

University of South Carolina Aiken

CSCI A591-PC

Dr. Ali AlSabeh

December 3, 2025

Scenario: Stonewall Consultants, Preventing Cross-Project Lateral Movement in LumaTech's OpenStack Cloud

Prerequisites:

- Basic Linux command-line knowledge
- Understanding of virtualization concepts
- Familiarity with OpenStack compute and identity operations
- Access to a laptop that can run VMWare Workstation Pro
- Snapshot of the provided DevStack OpenStack environment

Learning Objectives:

By the end of this lab, students will be able to:

- Identify misconfigurations in OpenStack networking that expose tenants to unauthorized internal communication.
- Demonstrate cross-project lateral movement using basic network tools inside cloud VMs.
- Design and implement proper network segmentation using Neutron networks, subnets, routers, and security groups.
- Validate isolation by testing traffic controls before and after remediation.
- Apply cloud security best practices to restrict east-west traffic and protect tenant workloads. [6]

Background:

In the previous engagement, LumaTech tasked Stonewall Consultants with implementing a strong identity and access management model across their OpenStack deployment. While role-based controls and MFA have now improved authentication and authorization, your team's follow-up assessment uncovered a different class of vulnerabilities in the networking layer.

Despite users being properly segmented into Dev and Test projects, both environments were provisioned on a shared provider network. This design flaw allows virtual machines from separate projects to communicate directly over the same Layer-2 segment. In effect, LumaTech unintentionally created a flat, multi-tenant network where workloads with separate business functions can still see, probe, or attack each other. [3]

As a result, a compromised VM in one project could perform reconnaissance, port scanning, or even connect to internal services in another project without ever being restricted by Keystone's IAM controls. [6]

Your Mission:

As Stonewall Consultants, you are now tasked with strengthening LumaTech's cloud security posture by eliminating cross-project lateral movement and enforcing proper tenant network isolation. You will:

- Assess the insecure shared network configuration and demonstrate the risks it introduces.
- Show how VMs in different projects can communicate despite identity separation.
- Re-architect the network to use project-specific Neutron networks and routers.
- Implement tighter security group rules to enforce least-privilege communication paths.
- Validate isolation by proving that unauthorized inter-tenant traffic is blocked after remediation.

By the end of this engagement, LumaTech should have clear boundaries between Dev and Test tenant networks, reduced east-west attack surface [6], and controls that prevent internal reconnaissance and pivoting across projects.

Section 0: Reviewing the current network

Before making any changes to LumaTech's cloud environment, the first step is to understand how their OpenStack deployment is currently structured. Although the organization has grown beyond its early "one-user-does-everything" phase, the underlying network design never evolved to match their new team structure or security requirements. What they have today is the accumulated result of hurried scaling: ad-hoc project creation, shared credentials, and a single provider network hosting all workloads, regardless of function or sensitivity. [3]

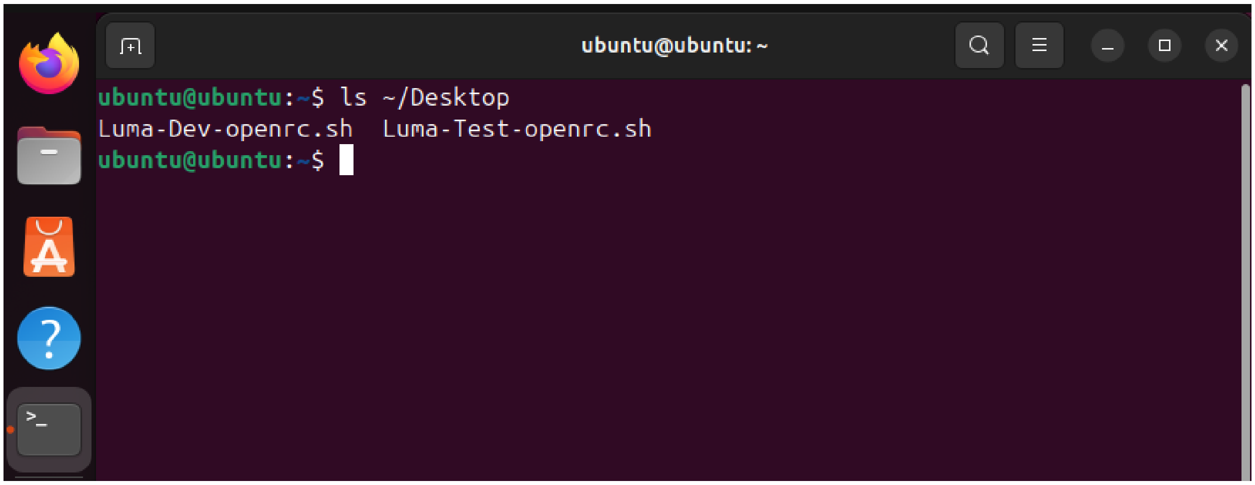
From a security perspective, this means we are walking into an environment where identity separation exists on paper, but network boundaries do not exist in practice. [5] The Dev and Test projects appear distinct in the dashboard, yet their instances ultimately sit on the same flat Layer-2 segment. This is exactly the kind of configuration drift that leads to unintentional trust relationships and silent lateral-movement paths inside a cloud. [3][5]

In this section, we establish the current state of LumaTech's environment. We inspect the RC files, confirm which credentials belong to which projects, and identify the networks each project is actually using. Before redesigning tenant networks or tightening security groups, we need a clear understanding of what we inherited and the risks it already exposes. This reconnaissance accomplishes two goals:

1. Reveal the misconfigurations that allow cross-project communication.
2. Create a baseline to measure the impact of the segmentation fixes later in the lab.

0.1 Inspecting the Test Project's Current Instances

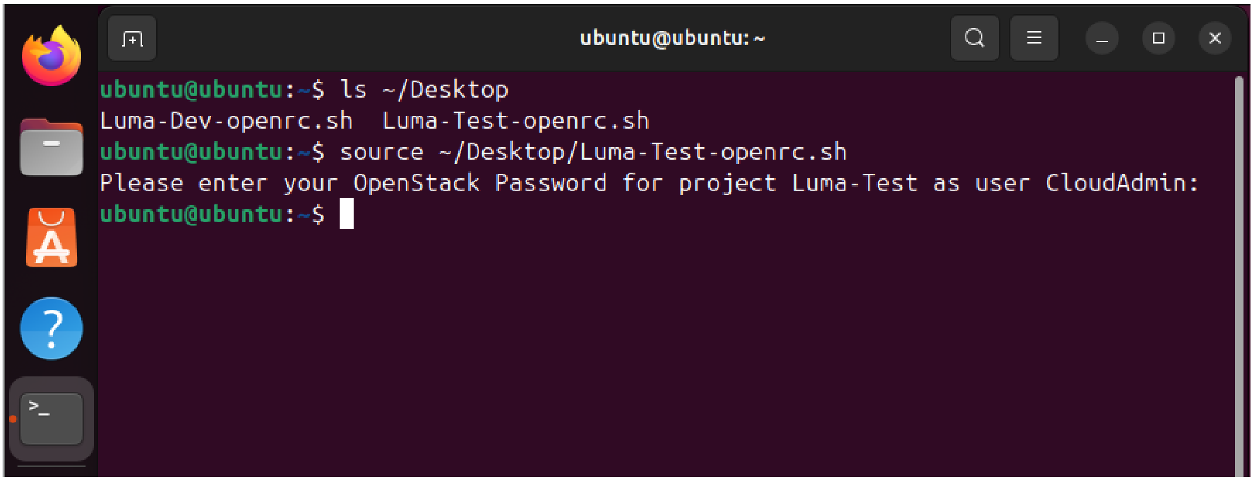
Step 1: Open the Ubuntu terminal on the DevStack VM, navigate to the desktop, and list the available RC files:



```
ubuntu@ubuntu:~$ ls ~/Desktop
Luma-Dev-openrc.sh  Luma-Test-openrc.sh
ubuntu@ubuntu:~$ 
```

Observe the provided RC files on the Desktop

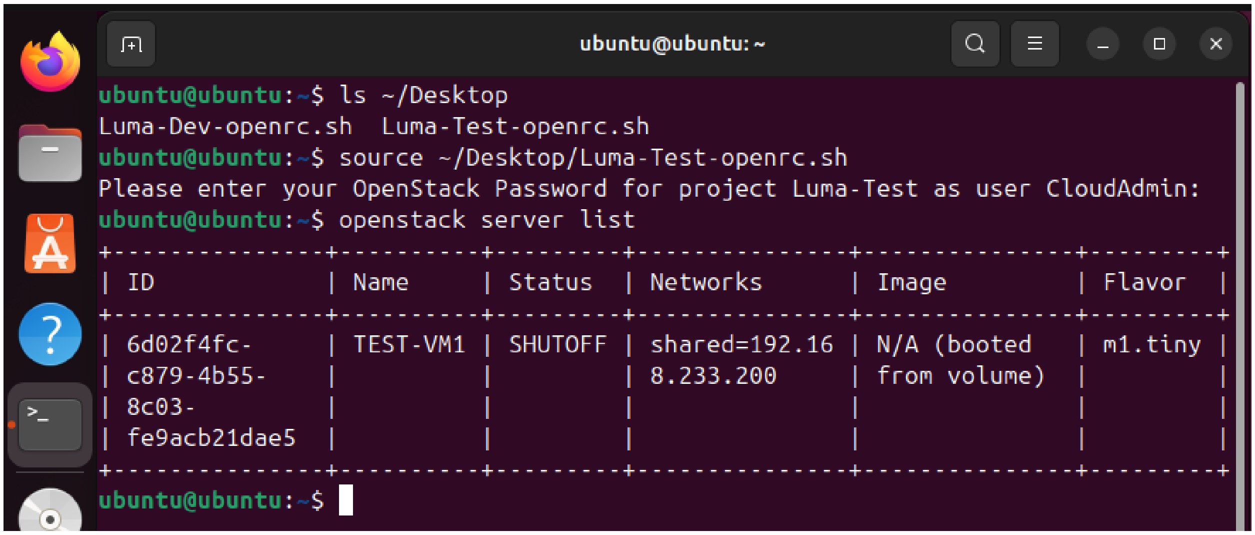
Step 2: Source the Test project credentials using "password" as the password:



```
ubuntu@ubuntu:~$ ls ~/Desktop
Luma-Dev-openrc.sh  Luma-Test-openrc.sh
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Test-openrc.sh
Please enter your OpenStack Password for project Luma-Test as user CloudAdmin:
ubuntu@ubuntu:~$ 
```

You are now authenticated as the CloudAdmin in the Luma-Test project

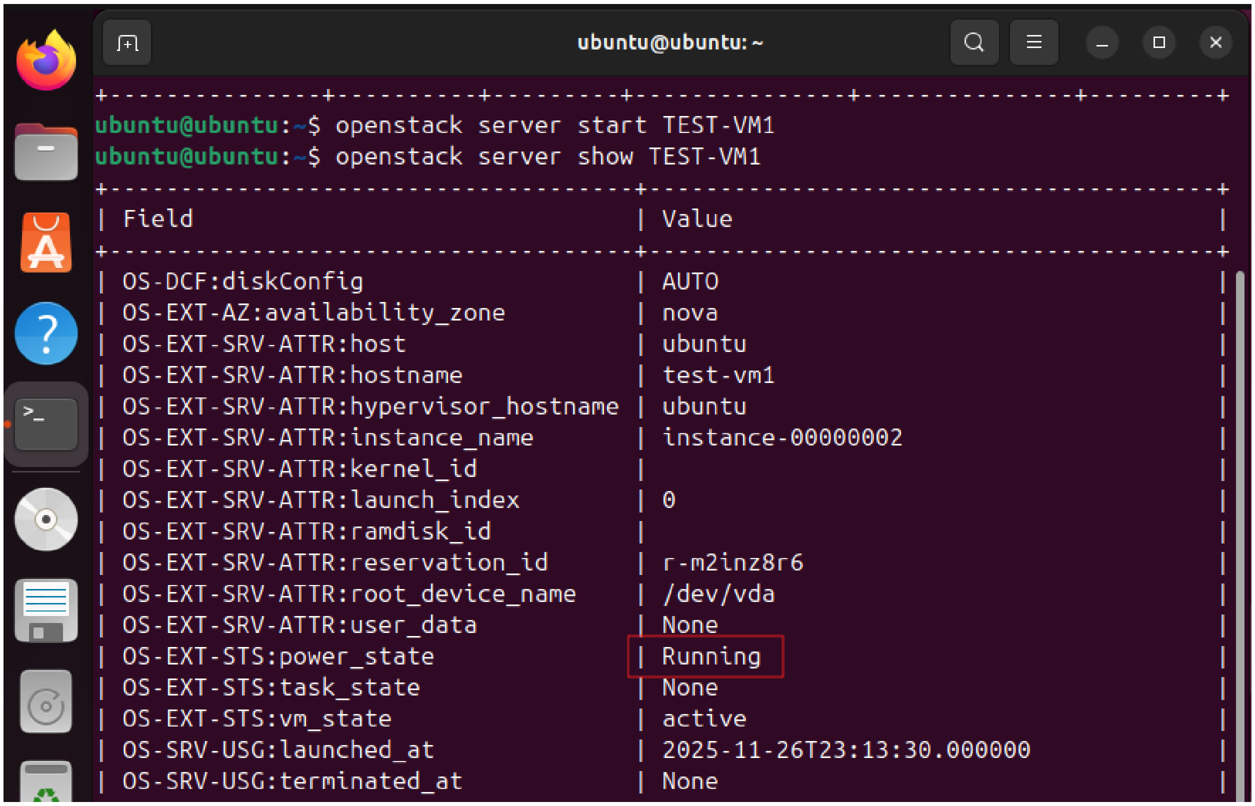
Step 3: List all instances in the Test project:



```
ubuntu@ubuntu:~$ ls ~/Desktop
Luma-Dev-openrc.sh  Luma-Test-openrc.sh
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Test-openrc.sh
Please enter your OpenStack Password for project Luma-Test as user CloudAdmin:
ubuntu@ubuntu:~$ openstack server list
+---------------+----------+---------+---------------+---------------+---------+
| ID            | Name     | Status  | Networks      | Image         | Flavor  |
+---------------+----------+---------+---------------+---------------+---------+
| 6d02f4fc-     | TEST-VM1 | SHUTOFF | shared=192.16 | N/A (booted   | m1.tiny |
| c879-4b55-    |          |         | 8.233.200     | from volume)  |         |
| 8c03-         |          |         |               |               |         |
| fe9acb21dae5  |          |         |               |               |         |
+---------------+----------+---------+---------------+---------------+---------+
ubuntu@ubuntu:~$
```

One instance is active in the Luma-Test project

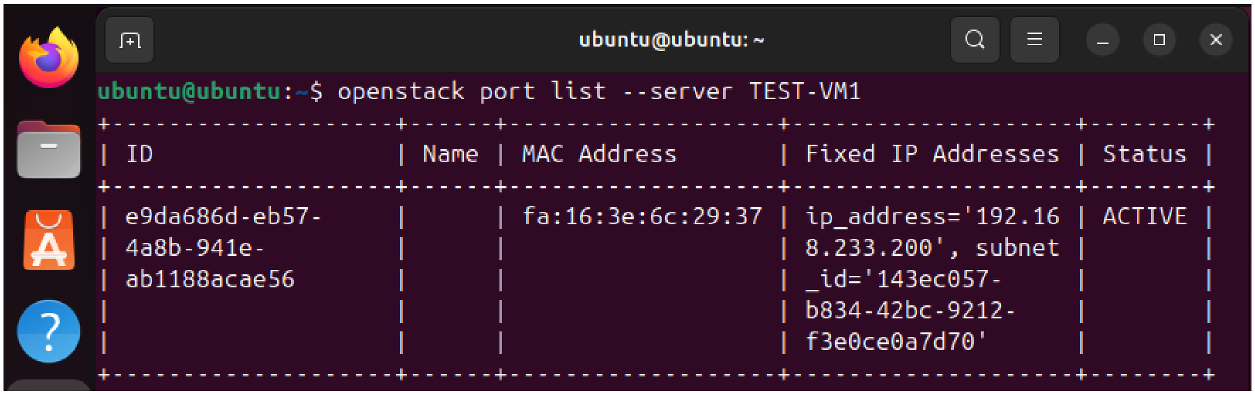
Step 4: Start the Test instance (if not already active), and confirm the instance is running:



```
+---------------+----------+---------+---------------+---------------+---------+
ubuntu@ubuntu:~$ openstack server start TEST-VM1
ubuntu@ubuntu:~$ openstack server show TEST-VM1
+-------------------------------------+--------------------------------------+
| Field                               | Value                                |
+-------------------------------------+--------------------------------------+
| OS-DCF:diskConfig                   | AUTO                                 |
| OS-EXT-AZ:availability_zone         | nova                                 |
| OS-EXT-SRV-ATTR:host                | ubuntu                               |
| OS-EXT-SRV-ATTR:hostname            | test-vm1                             |
| OS-EXT-SRV-ATTR:hypervisor_hostname | ubuntu                               |
| OS-EXT-SRV-ATTR:instance_name       | instance-00000002                    |
| OS-EXT-SRV-ATTR:kernel_id           |                                      |
| OS-EXT-SRV-ATTR:launch_index        | 0                                    |
| OS-EXT-SRV-ATTR:ramdisk_id          |                                      |
| OS-EXT-SRV-ATTR:reservation_id      | r-m2inz8r6                           |
| OS-EXT-SRV-ATTR:root_device_name    | /dev/vda                             |
| OS-EXT-SRV-ATTR:user_data           | None                                 |
| OS-EXT-STS:power_state              | Running                              |
| OS-EXT-STS:task_state               | None                                 |
| OS-EXT-STS:vm_state                 | active                               |
| OS-SRV-USG:launched_at              | 2025-11-26T23:13:30.000000           |
| OS-SRV-USG:terminated_at            | None                                 |
```

As you can see, the power_state is currently showing Running

Step 5: Identify which network the Test VM is connected to:

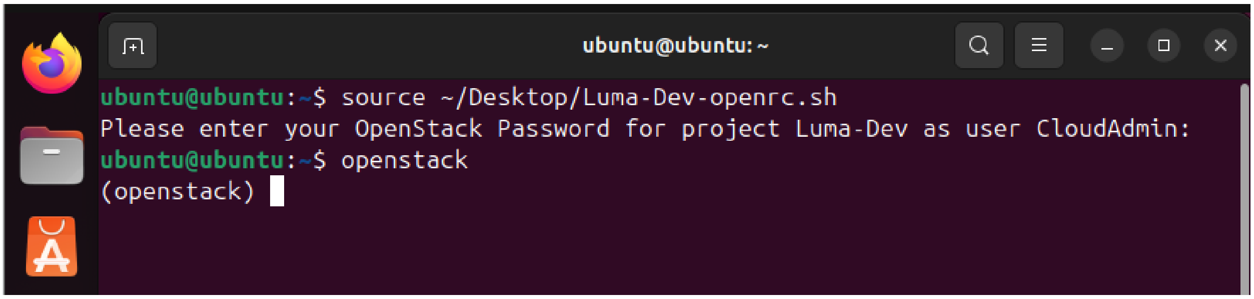


```
ubuntu@ubuntu:~$ openstack port list --server TEST-VM1
+--------------------+-----+-------------------+-------------------+--------+
| ID                 | Name | MAC Address      | Fixed IP Addresses | Status |
+--------------------+-----+-------------------+-------------------+--------+
| e9da686d-eb57-     |      | fa:16:3e:6c:29:37 | ip_address='192.16 | ACTIVE |
| 4a8b-941e-         |      |                   | 8.233.200', subnet |        |
| ab1188acae56       |      |                   | _id='143ec057-     |        |
|                    |      |                   | b834-42bc-9212-    |        |
|                    |      |                   | f3e0ce0a7d70'      |        |
+--------------------+-----+-------------------+-------------------+--------+
```

Take note of the subnet_id for later

0.3 Repeating the Investigation for the Dev Project

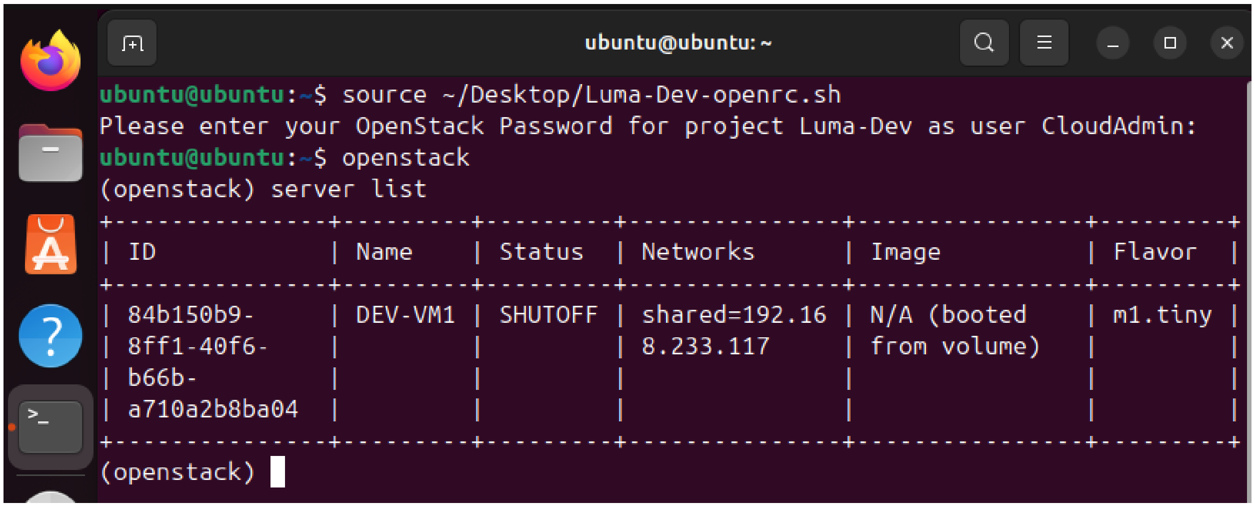
Step 6: Open a new terminal and source the Dev project credentials using the same password from section 0.1. This time, use the OpenStack CLI:



```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Dev-openrc.sh
Please enter your OpenStack Password for project Luma-Dev as user CloudAdmin:
ubuntu@ubuntu:~$ openstack
(openstack) 
```

You are now logged in as the CloudAdmin on the Luma-Dev project

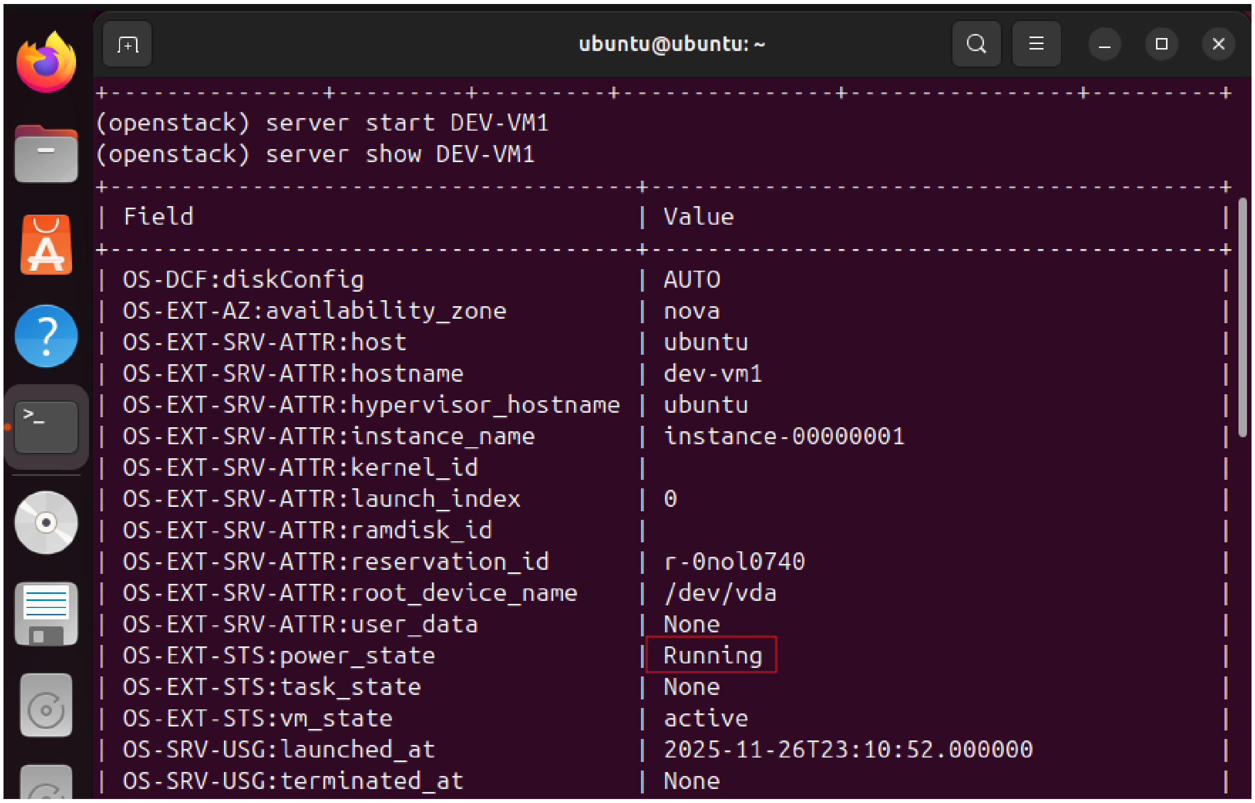
Step 7: List Dev instances:



```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Dev-openrc.sh
Please enter your OpenStack Password for project Luma-Dev as user CloudAdmin:
ubuntu@ubuntu:~$ openstack
(openstack) server list
+---------------+---------+---------+----------------+----------------+---------+
| ID            | Name    | Status  | Networks       | Image          | Flavor  |
+---------------+---------+---------+----------------+----------------+---------+
| 84b150b9-     | DEV-VM1 | SHUTOFF | shared=192.16  | N/A (booted    | m1.tiny |
| 8ff1-40f6-    |         |         | 8.233.117      | from volume)   |         |
| b66b-         |         |         |                |                |         |
| a710a2b8ba04  |         |         |                |                |         |
+---------------+---------+---------+----------------+----------------+---------+
(openstack) 
```

One instance is active in the Luma-Dev project

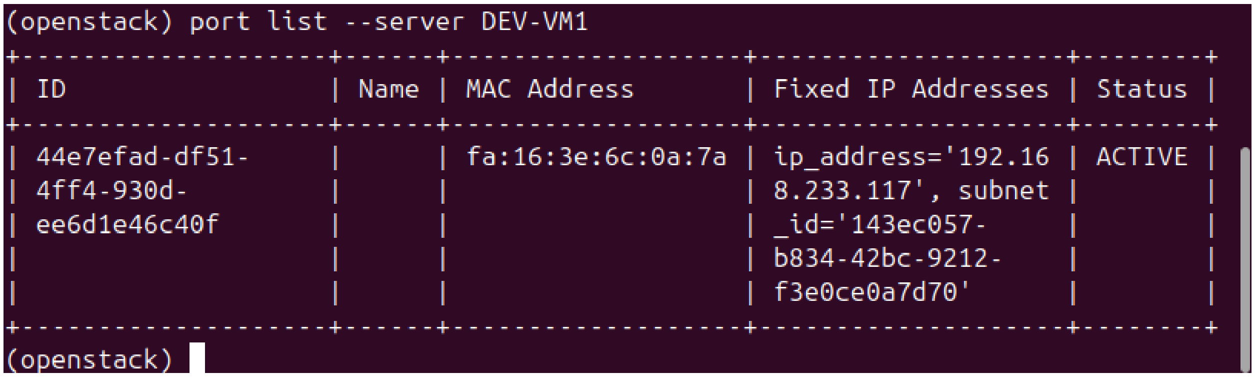
Step 8: Start the Dev VM if needed, and confirm the instance details:



```
+---------------+---------+---------+---------------+---------------+---------+
(openstack) server start DEV-VM1
(openstack) server show DEV-VM1
+-------------------------------------+--------------------------------------+
| Field                               | Value                                |
+-------------------------------------+--------------------------------------+
| OS-DCF:diskConfig                   | AUTO                                 |
| OS-EXT-AZ:availability_zone         | nova                                 |
| OS-EXT-SRV-ATTR:host                | ubuntu                               |
| OS-EXT-SRV-ATTR:hostname            | dev-vm1                              |
| OS-EXT-SRV-ATTR:hypervisor_hostname | ubuntu                               |
| OS-EXT-SRV-ATTR:instance_name       | instance-00000001                    |
| OS-EXT-SRV-ATTR:kernel_id           |                                      |
| OS-EXT-SRV-ATTR:launch_index        | 0                                    |
| OS-EXT-SRV-ATTR:ramdisk_id          |                                      |
| OS-EXT-SRV-ATTR:reservation_id      | r-0nol0740                           |
| OS-EXT-SRV-ATTR:root_device_name    | /dev/vda                             |
| OS-EXT-SRV-ATTR:user_data           | None                                 |
| OS-EXT-STS:power_state              | Running                              |
| OS-EXT-STS:task_state               | None                                 |
| OS-EXT-STS:vm_state                 | active                               |
| OS-SRV-USG:launched_at              | 2025-11-26T23:10:52.000000           |
| OS-SRV-USG:terminated_at            | None                                 |
```

The power_state is now showing Running

Step 9: View the network that the Dev instance is attached to:

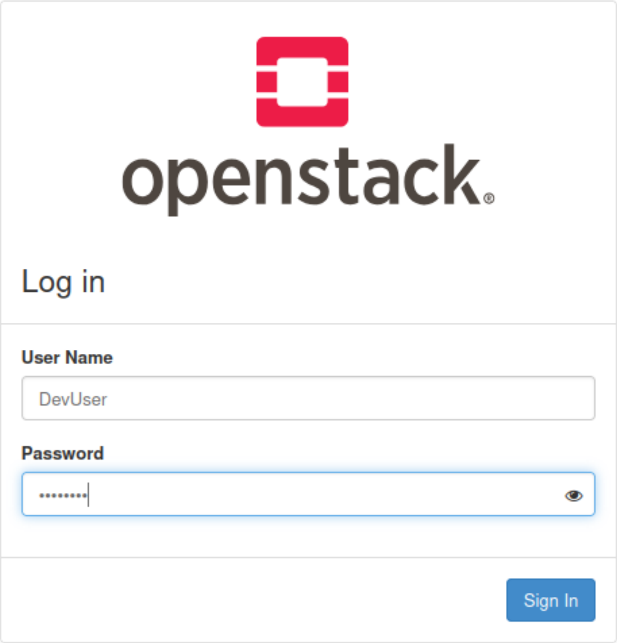


```
(openstack) port list --server DEV-VM1
+----------------------+------+-------------------+--------------------+--------+
| ID                   | Name | MAC Address       | Fixed IP Addresses | Status |
+----------------------+------+-------------------+--------------------+--------+
| 44e7efad-df51-       |      | fa:16:3e:6c:0a:7a | ip_address='192.16 | ACTIVE |
| 4ff4-930d-           |      |                   | 8.233.117', subnet |        |
| ee6d1e46c40f         |      |                   | _id='143ec057-     |        |
|                      |      |                   | b834-42bc-9212-    |        |
|                      |      |                   | f3e0ce0a7d70'      |        |
+----------------------+------+-------------------+--------------------+--------+
(openstack) 
```

Compare the subnet_id to the subnet_id from TEST-VM1

0.4 Validating Cross-Project Communication in Horizon

Step 10: Log in to the OpenStack Horizon dashboard with the credentials "DevUser":"password":



Log in

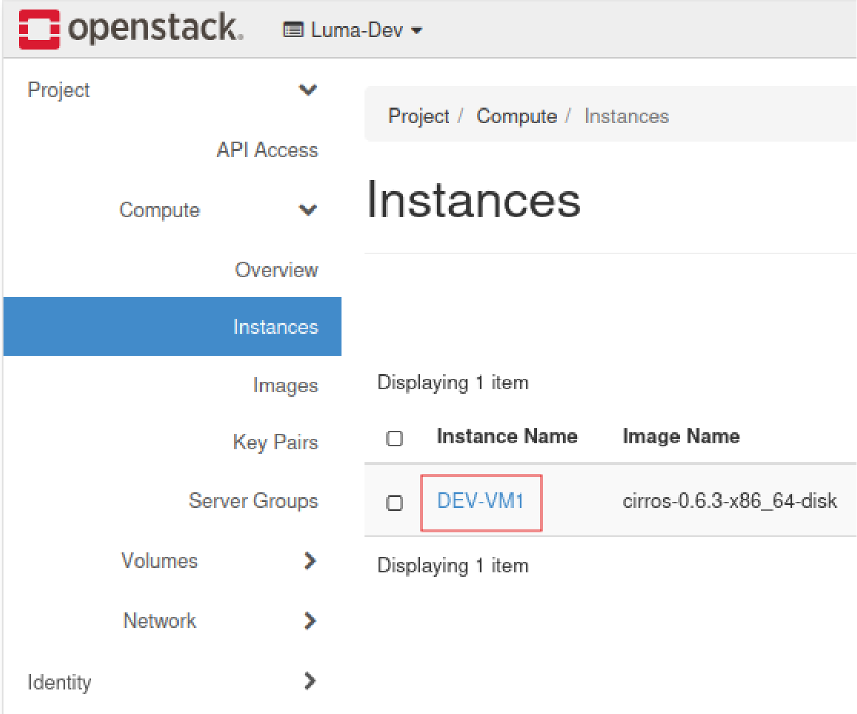
User Name

DevUser

Password

••••••••

Step 11: Open the VM's console using Project → Compute → Instances then click the instance's name:



Project / Compute / Instances

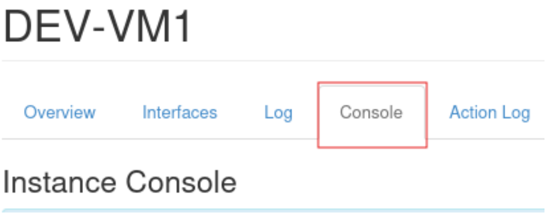
Instances

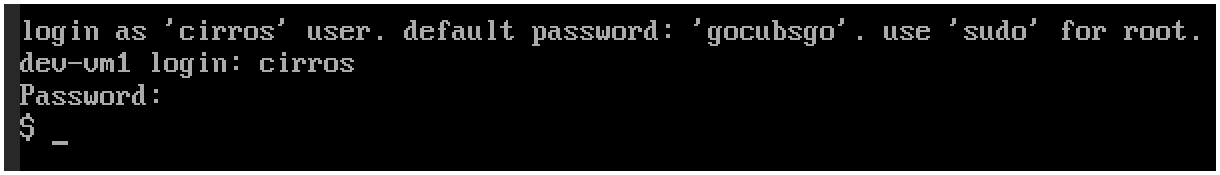
Displaying 1 item

□	Instance Name	Image Name
□	DEV-VM1	cirros-0.6.3-x86_64-disk

Displaying 1 item

Step 12: Click the Console tab, and use the credentials provided by the cirros image to login to the VM:

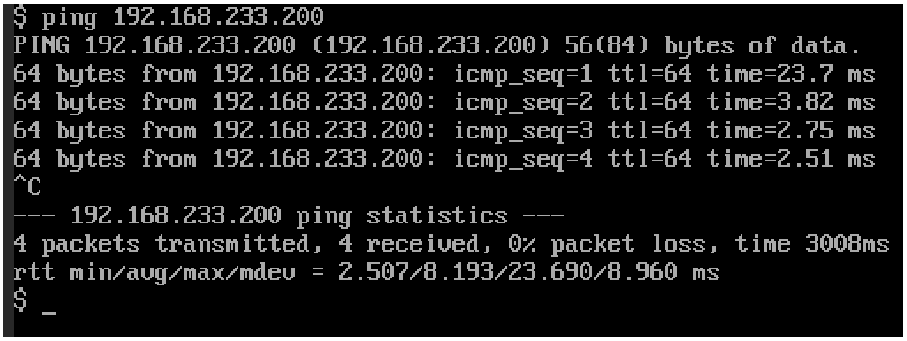




```
login as 'cirros' user. default password: 'gocubsgo'. use 'sudo' for root.
dev-vm1 login: cirros
Password:
$ _
```

The login and password for root is provided in the console

Step 13: From the Dev VM, ping the Test VM's internal IP (after 4 packets are sent, press Ctrl+C to stop pinging):

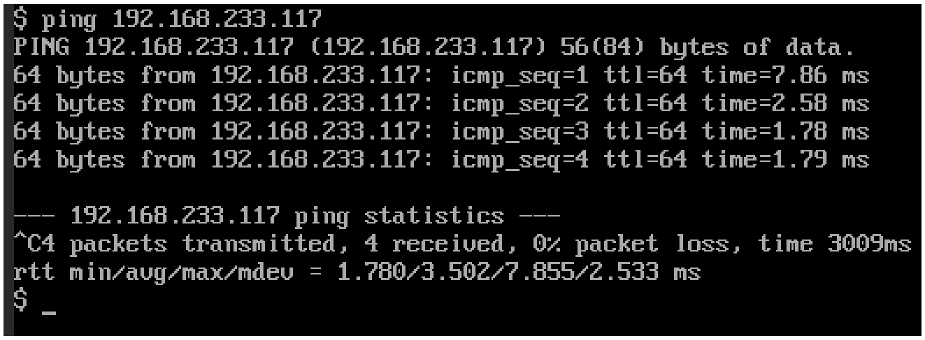


```
$ ping 192.168.233.200
PING 192.168.233.200 (192.168.233.200) 56(84) bytes of data.
64 bytes from 192.168.233.200: icmp_seq=1 ttl=64 time=23.7 ms
64 bytes from 192.168.233.200: icmp_seq=2 ttl=64 time=3.82 ms
64 bytes from 192.168.233.200: icmp_seq=3 ttl=64 time=2.75 ms
64 bytes from 192.168.233.200: icmp_seq=4 ttl=64 time=2.51 ms
^C
--- 192.168.233.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 2.507/8.193/23.690/8.960 ms
$ _
```

The pings are successful

Step 14: After signing out of the Horizon Dashboard, repeat steps 10 through 12 using the credentials "QAUser":" password".

Step 15: From the Test VM, ping the Dev VM's internal IP (after 4 packets are sent, press Ctrl+C to stop pinging):



```
$ ping 192.168.233.117
PING 192.168.233.117 (192.168.233.117) 56(84) bytes of data.
64 bytes from 192.168.233.117: icmp_seq=1 ttl=64 time=7.86 ms
64 bytes from 192.168.233.117: icmp_seq=2 ttl=64 time=2.58 ms
64 bytes from 192.168.233.117: icmp_seq=3 ttl=64 time=1.78 ms
64 bytes from 192.168.233.117: icmp_seq=4 ttl=64 time=1.79 ms

--- 192.168.233.117 ping statistics ---
^C4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 1.780/3.502/7.855/2.533 ms
$ _
```

The pings were successful in the other direction as well

Step 16: Observe that the pings succeed because both VMs are on the same provider network with permissive default security groups.

0.5 Section Summary

Document your findings:

a. Both projects share a single provider network.

b. Default security groups allow egress and do not block ICMP between tenants.

c. Identity separation does not prevent network-level communication. [6]

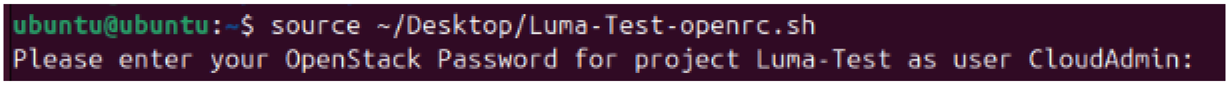
This completes the baseline assessment of LumaTech’s current cloud environment.

Section 1: Segregating Cloud Resources for Least Privilege

As part of our assessment of LumaTech’s cloud posture, our team’s first objective is to establish clear network boundaries between business units. This phase focuses on segmenting the environment into dedicated tenant networks that prevent accidental or unauthorized cross-communication. By aligning these segments with LumaTech’s internal organizational structure, we ensure that each department’s workloads operate within controlled, isolated spaces that reflect industry best practices for least-privilege design. [1],[2]

1.1 Creating a Dedicated Network for the Test Project

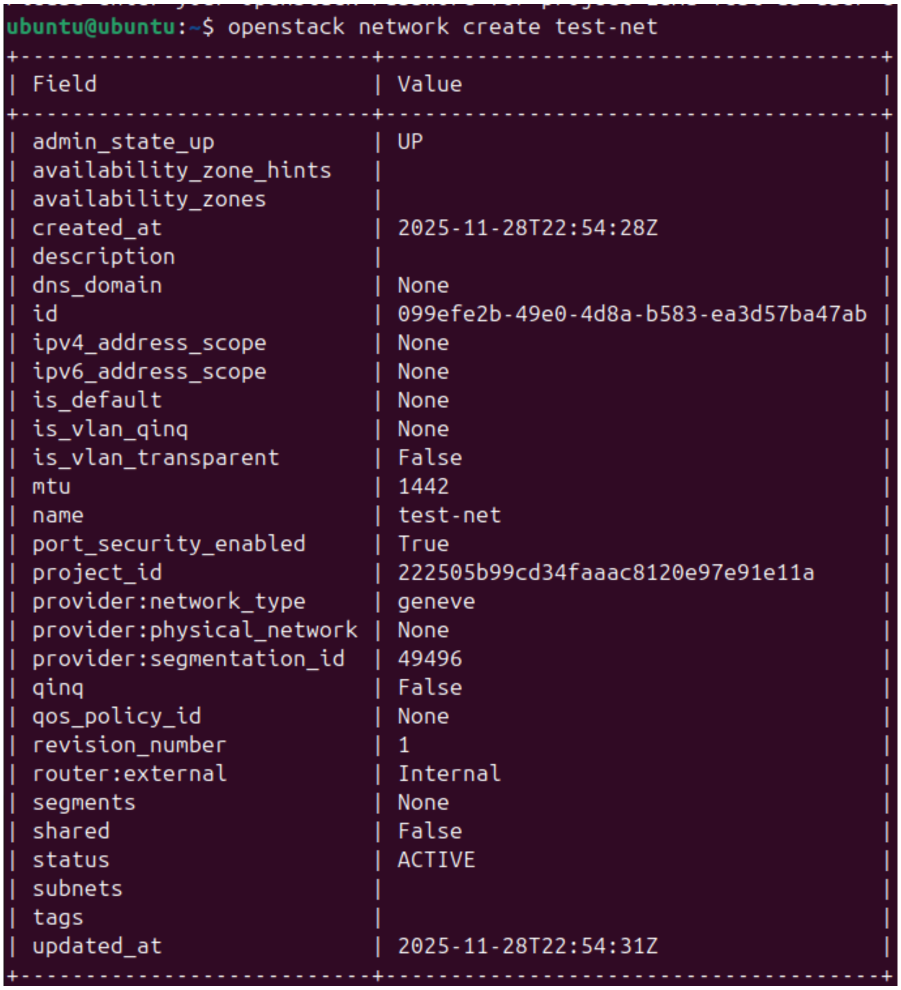
Step 1: Source the Test project credentials:



```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Test-openrc.sh
Please enter your OpenStack Password for project Luma-Test as user CloudAdmin:
```

Password: “password”

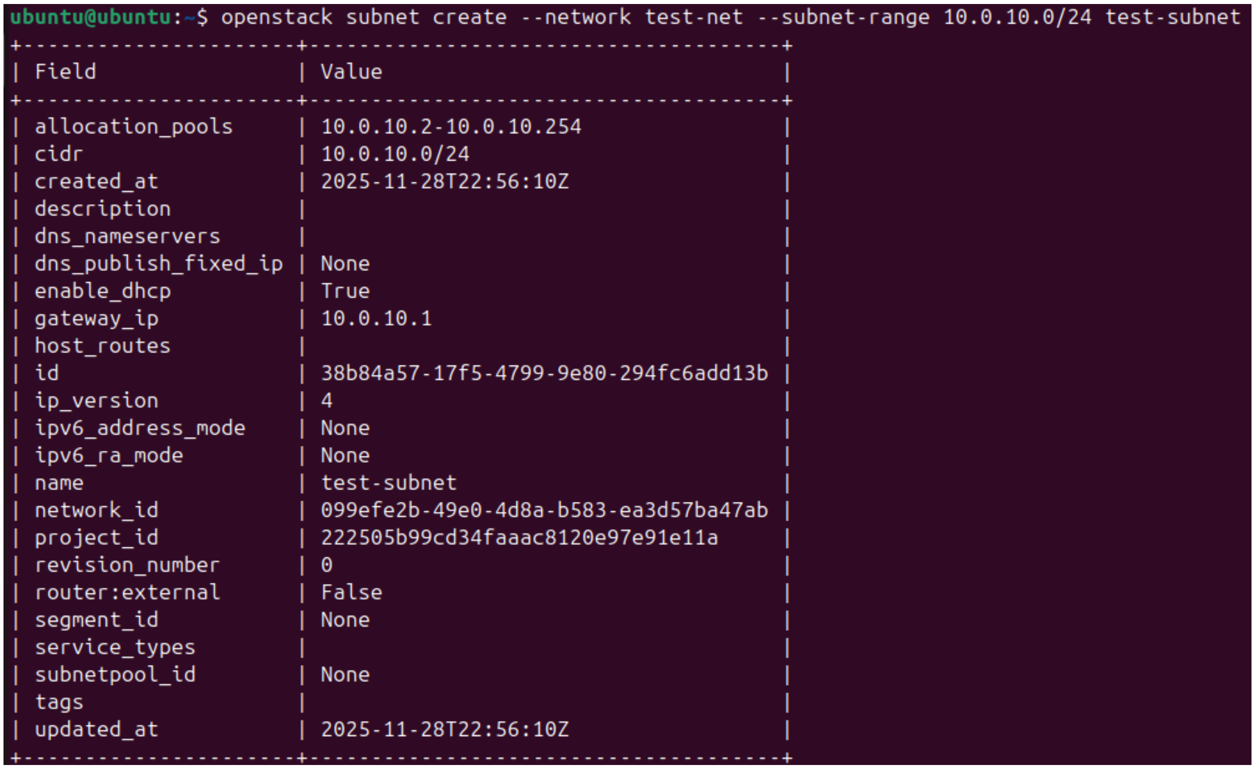
Step 2: Create a new isolated network for the Test project:



```
ubuntu@ubuntu:~$ openstack network create test-net
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | UP                                   |
| availability_zone_hints   |                                      |
| availability_zones        |                                      |
| created_at                | 2025-11-28T22:54:28Z                 |
| description               |                                      |
| dns_domain                | None                                 |
| id                        | 099efe2b-49e0-4d8a-b583-ea3d57ba47ab |
| ipv4_address_scope        | None                                 |
| ipv6_address_scope        | None                                 |
| is_default                | None                                 |
| is_vlan_qinq              | None                                 |
| is_vlan_transparent       | False                                |
| mtu                       | 1442                                 |
| name                      | test-net                             |
| port_security_enabled     | True                                 |
| project_id                | 222505b99cd34faaac8120e97e91e11a     |
| provider:network_type     | geneve                               |
| provider:physical_network | None                                 |
| provider:segmentation_id  | 49496                                |
| qinq                      | False                                |
| qos_policy_id             | None                                 |
| revision_number           | 1                                    |
| router:external           | Internal                             |
| segments                  | None                                 |
| shared                    | False                                |
| status                    | ACTIVE                               |
| subnets                   |                                      |
| tags                      |                                      |
| updated_at                | 2025-11-28T22:54:31Z                 |
+---------------------------+--------------------------------------+
```

The test network is now created

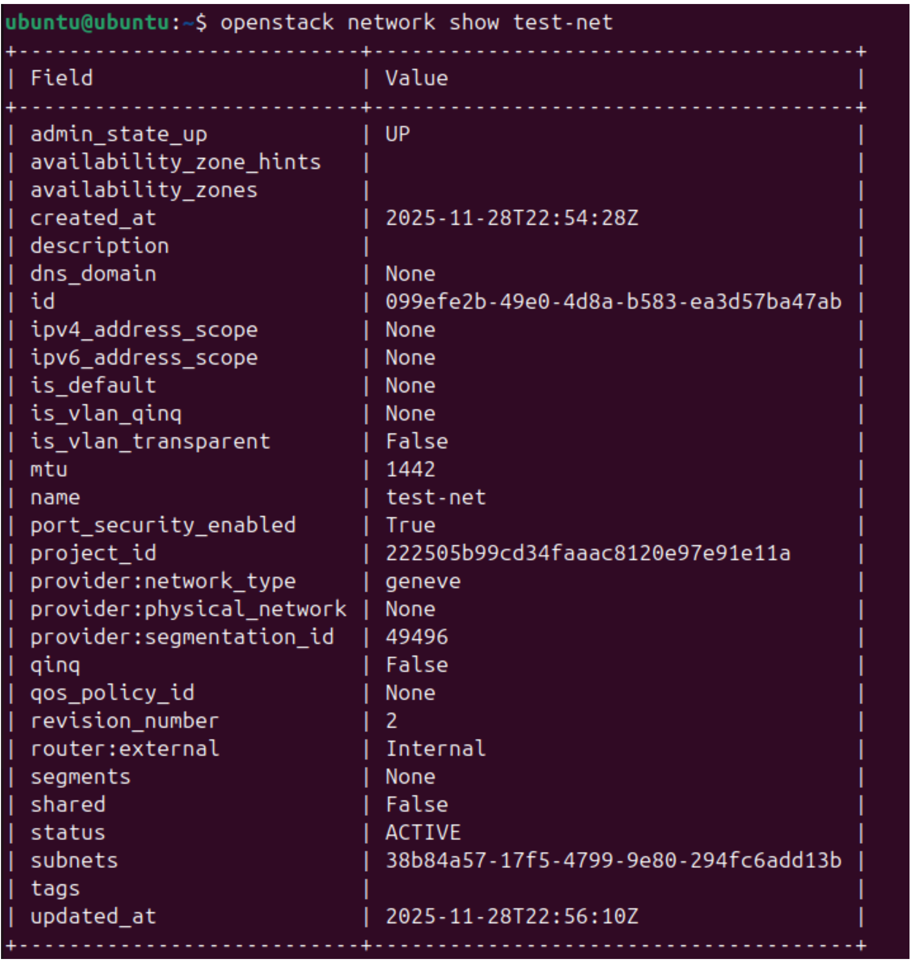
Step 3: Add a subnet to this network (CIDR example: 10.0.10.0/24):



```
ubuntu@ubuntu:~$ openstack subnet create --network test-net --subnet-range 10.0.10.0/24 test-subnet
+----------------------+--------------------------------------+
| Field                | Value                                |
+----------------------+--------------------------------------+
| allocation_pools     | 10.0.10.2-10.0.10.254                |
| cidr                 | 10.0.10.0/24                         |
| created_at           | 2025-11-28T22:56:10Z                 |
| description          |                                      |
| dns_nameservers      |                                      |
| dns_publish_fixed_ip | None                                 |
| enable_dhcp          | True                                 |
| gateway_ip           | 10.0.10.1                            |
| host_routes          |                                      |
| id                   | 38b84a57-17f5-4799-9e80-294fc6add13b |
| ip_version           | 4                                    |
| ipv6_address_mode    | None                                 |
| ipv6_ra_mode         | None                                 |
| name                 | test-subnet                          |
| network_id           | 099efe2b-49e0-4d8a-b583-ea3d57ba47ab |
| project_id           | 222505b99cd34faaac8120e97e91e11a     |
| revision_number      | 0                                    |
| router:external      | False                                |
| segment_id           | None                                 |
| service_types        |                                      |
| subnetpool_id        | None                                 |
| tags                 |                                      |
| updated_at           | 2025-11-28T22:56:10Z                 |
+----------------------+--------------------------------------+
```

The new subnet is now created

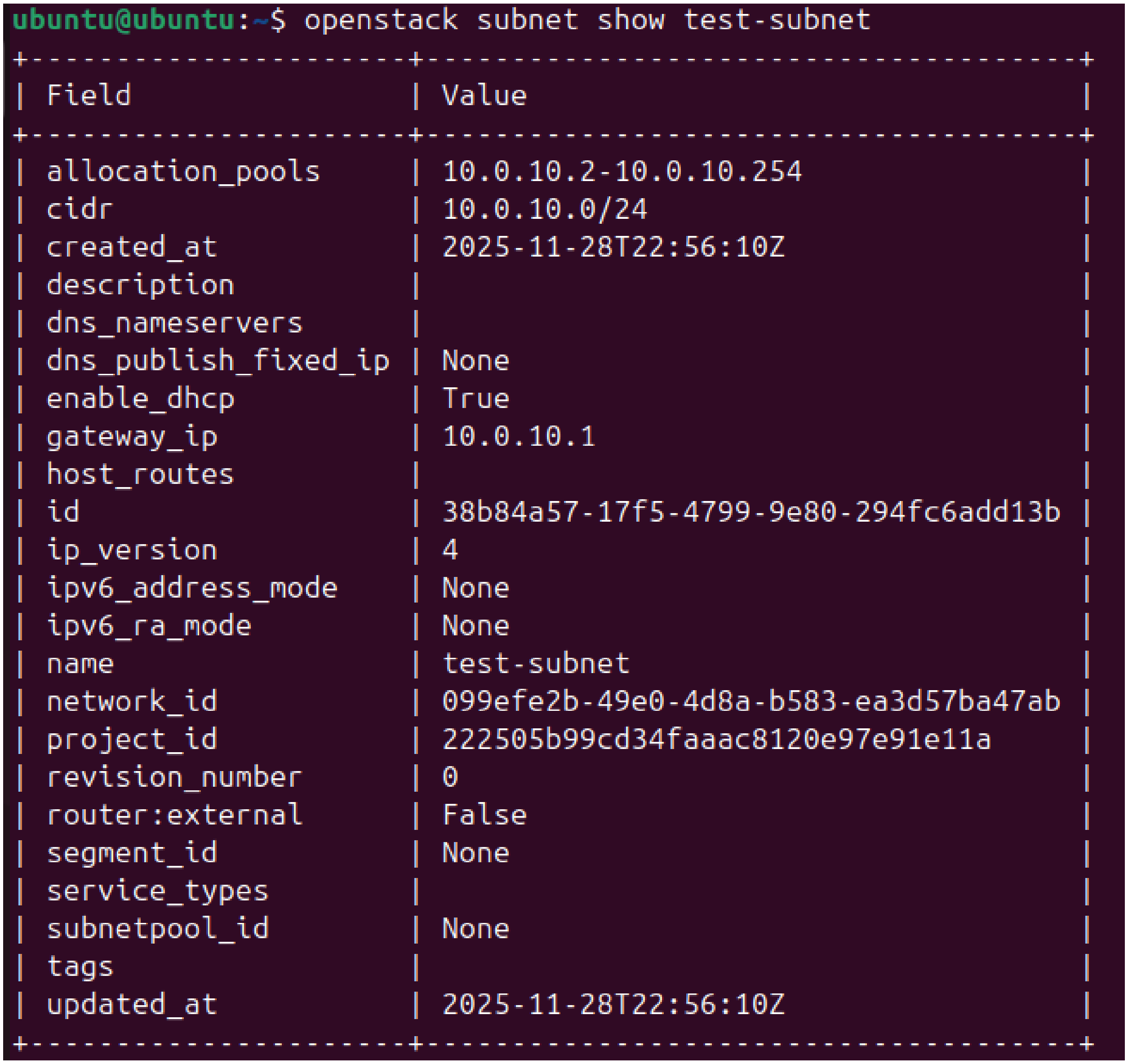
Step 4: Verify the new network and subnet exist:



```
ubuntu@ubuntu:~$ openstack network show test-net
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | UP                                   |
| availability_zone_hints   |                                      |
| availability_zones        |                                      |
| created_at                | 2025-11-28T22:54:28Z                 |
| description               |                                      |
| dns_domain                | None                                 |
| id                        | 099efe2b-49e0-4d8a-b583-ea3d57ba47ab |
| ipv4_address_scope        | None                                 |
| ipv6_address_scope        | None                                 |
| is_default                | None                                 |
| is_vlan_qinq              | None                                 |
| is_vlan_transparent       | False                                |
| mtu                       | 1442                                 |
| name                      | test-net                             |
| port_security_enabled     | True                                 |
| project_id                | 222505b99cd34faaac8120e97e91e11a     |
| provider:network_type     | geneve                               |
| provider:physical_network | None                                 |
| provider:segmentation_id  | 49496                                |
| qinq                      | False                                |
| qos_policy_id             | None                                 |
| revision_number           | 2                                    |
| router:external           | Internal                             |
| segments                  | None                                 |
| shared                    | False                                |
| status                    | ACTIVE                               |
| subnets                   | 38b84a57-17f5-4799-9e80-294fc6add13b |
| tags                      |                                      |
| updated_at                | 2025-11-28T22:56:10Z                 |
+---------------------------+--------------------------------------+
```

o

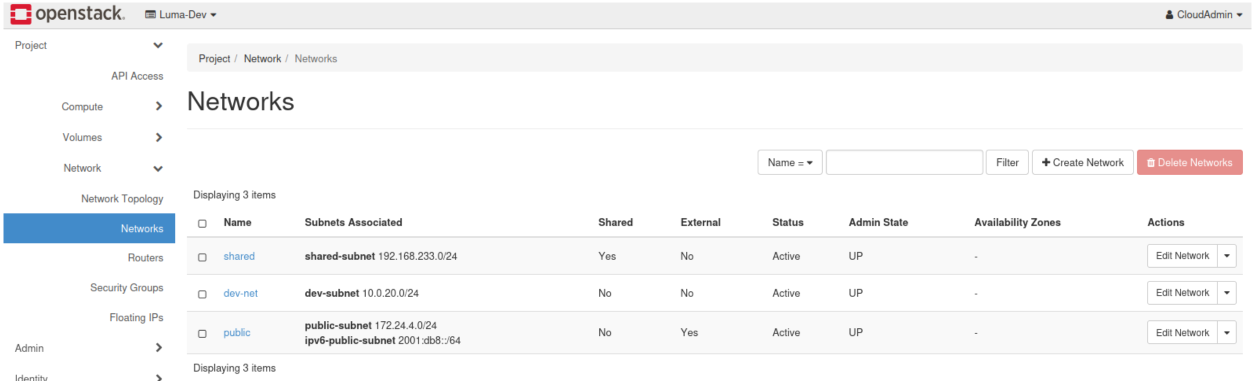
The test network exists



```
ubuntu@ubuntu:~$ openstack subnet show test-subnet
+----------------------+--------------------------------------+
| Field                | Value                                |
+----------------------+--------------------------------------+
| allocation_pools     | 10.0.10.2-10.0.10.254                |
| cidr                 | 10.0.10.0/24                         |
| created_at           | 2025-11-28T22:56:10Z                 |
| description          |                                      |
| dns_nameservers      |                                      |
| dns_publish_fixed_ip | None                                 |
| enable_dhcp          | True                                 |
| gateway_ip           | 10.0.10.1                            |
| host_routes          |                                      |
| id                   | 38b84a57-17f5-4799-9e80-294fc6add13b |
| ip_version           | 4                                    |
| ipv6_address_mode    | None                                 |
| ipv6_ra_mode         | None                                 |
| name                 | test-subnet                          |
| network_id           | 099efe2b-49e0-4d8a-b583-ea3d57ba47ab |
| project_id           | 222505b99cd34faaac8120e97e91e11a     |
| revision_number      | 0                                    |
| router:external      | False                                |
| segment_id           | None                                 |
| service_types        |                                      |
| subnetpool_id        | None                                 |
| tags                 |                                      |
| updated_at           | 2025-11-28T22:56:10Z                 |
+----------------------+--------------------------------------+
```

The subnet exists as well

Step 5: Confirm that it is visible only to the Test project:



Networks

Name = ▾ | Filter | ✚ Create Network | Delete Networks

Displaying 3 items

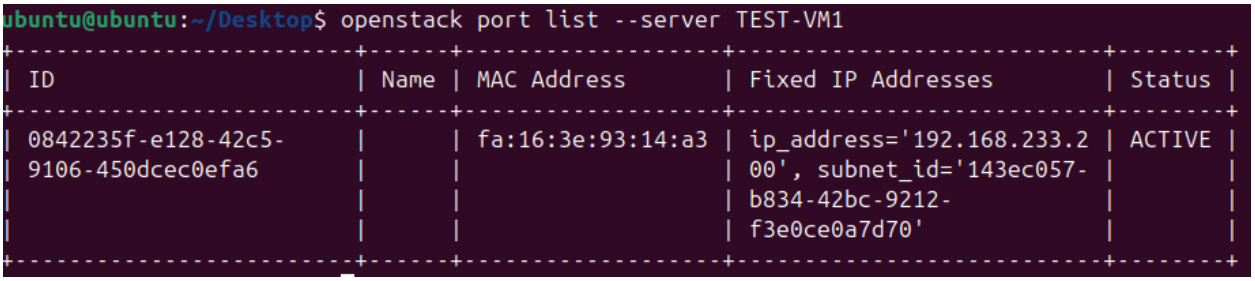
□	Name	Subnets Associated	Shared	External	Status	Admin State	Availability Zones	Actions
□	shared	**shared-subnet** 192.168.233.0/24	Yes	No	Active	UP	-	Edit Network ▾
□	dev-net	**dev-subnet** 10.0.20.0/24	No	No	Active	UP	-	Edit Network ▾
□	public	**public-subnet** 172.24.4.0/24 **ipv6-public-subnet** 2001:db8::/64	No	Yes	Active	UP	-	Edit Network ▾

Displaying 3 items

The dev environment cannot see "test-net"

1.2 Moving the Test VM Off the Shared Provider Network

Step 6: List the Test VM's current ports:



```
ubuntu@ubuntu:~/Desktop$ openstack port list --server TEST-VM1
+--------------------------+------+-------------------+---------------------------+--------+
| ID                       | Name | MAC Address       | Fixed IP Addresses        | Status |
+--------------------------+------+-------------------+---------------------------+--------+
| 0842235f-e128-42c5-      |      | fa:16:3e:93:14:a3 | ip_address='192.168.233.2 | ACTIVE |
| 9106-450dcec0efa6        |      |                   | 00', subnet_id='143ec057- |        |
|                          |      |                   | b834-42bc-9212-           |        |
|                          |      |                   | f3e0ce0a7d70'             |        |
+--------------------------+------+-------------------+---------------------------+--------+
```

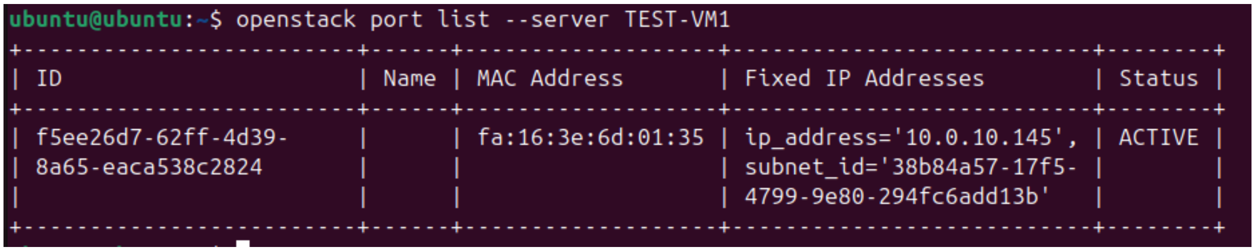
Step 6: Detach the VM from the provider network by typing "openstack server remove network TEST-VM1 shared" into the terminal.

(No Output is displayed)

Step 7: Attach the VM to the new Test network by typing "openstack server add network TEST-VM1 test-net" into the terminal.

(No Output is displayed)

Step 8: Verify the updated network attachment:

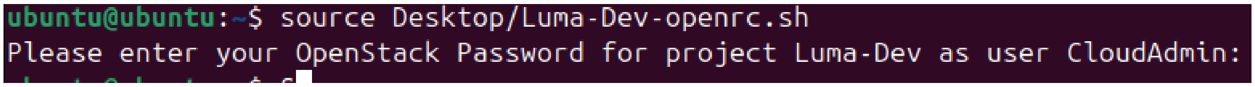


```
ubuntu@ubuntu:~$ openstack port list --server TEST-VM1
+--------------------------+------+-------------------+---------------------------+--------+
| ID                       | Name | MAC Address       | Fixed IP Addresses        | Status |
+--------------------------+------+-------------------+---------------------------+--------+
| f5ee26d7-62ff-4d39-      |      | fa:16:3e:6d:01:35 | ip_address='10.0.10.145', | ACTIVE |
| 8a65-eaca538c2824        |      |                   | subnet_id='38b84a57-17f5- |        |
|                          |      |                   | 4799-9e80-294fc6add13b'   |        |
+--------------------------+------+-------------------+---------------------------+--------+
```

The IP is 10.0.10.145. Your IP may vary but take note of your IP address. This confirms that we have made it to the test subnet [3] (10.0.10.)*

1.3 Creating a Dedicated Network for the Dev Project

Step 9: Switch to the Dev project credentials:



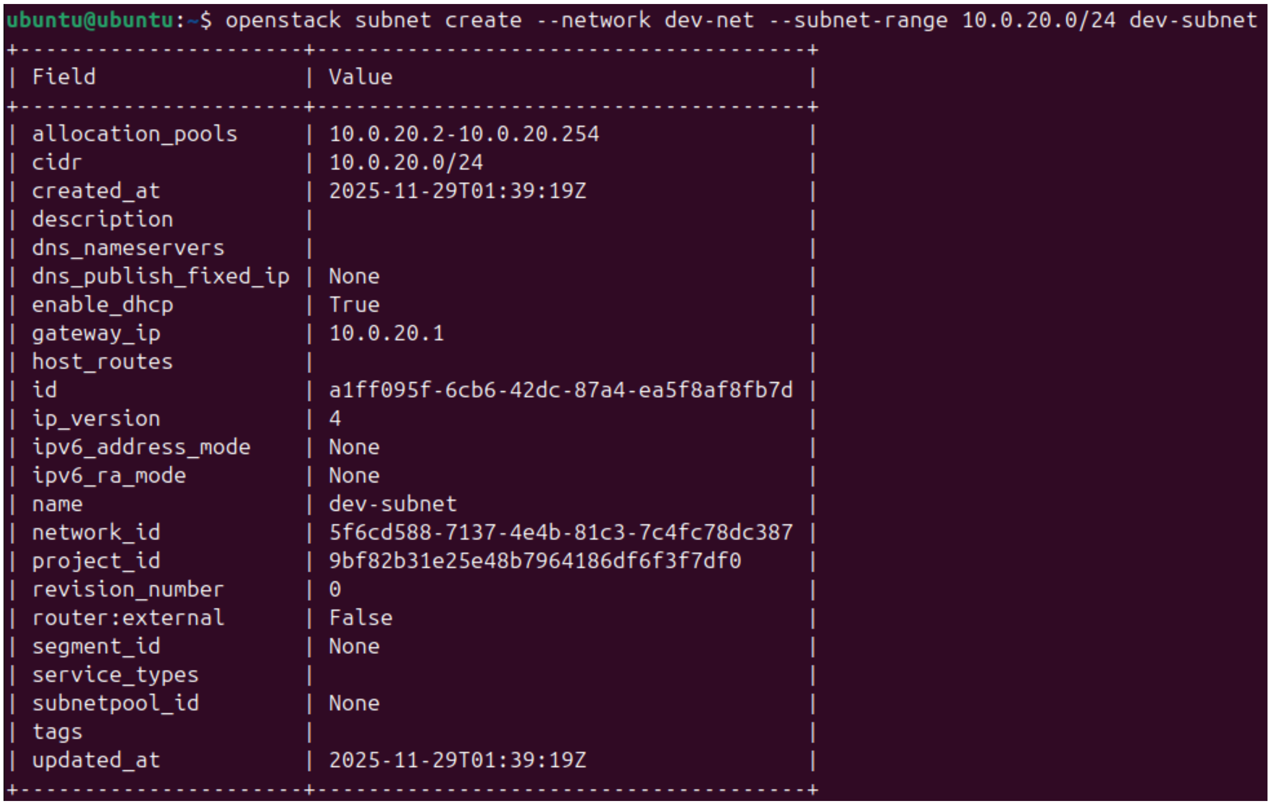
```
ubuntu@ubuntu:~$ source Desktop/Luma-Dev-openrc.sh
Please enter your OpenStack Password for project Luma-Dev as user CloudAdmin:
```

Password: “password”

Step 10: Create the Dev network by typing “openstack network create dev-net" into the terminal.

(No Output is displayed)

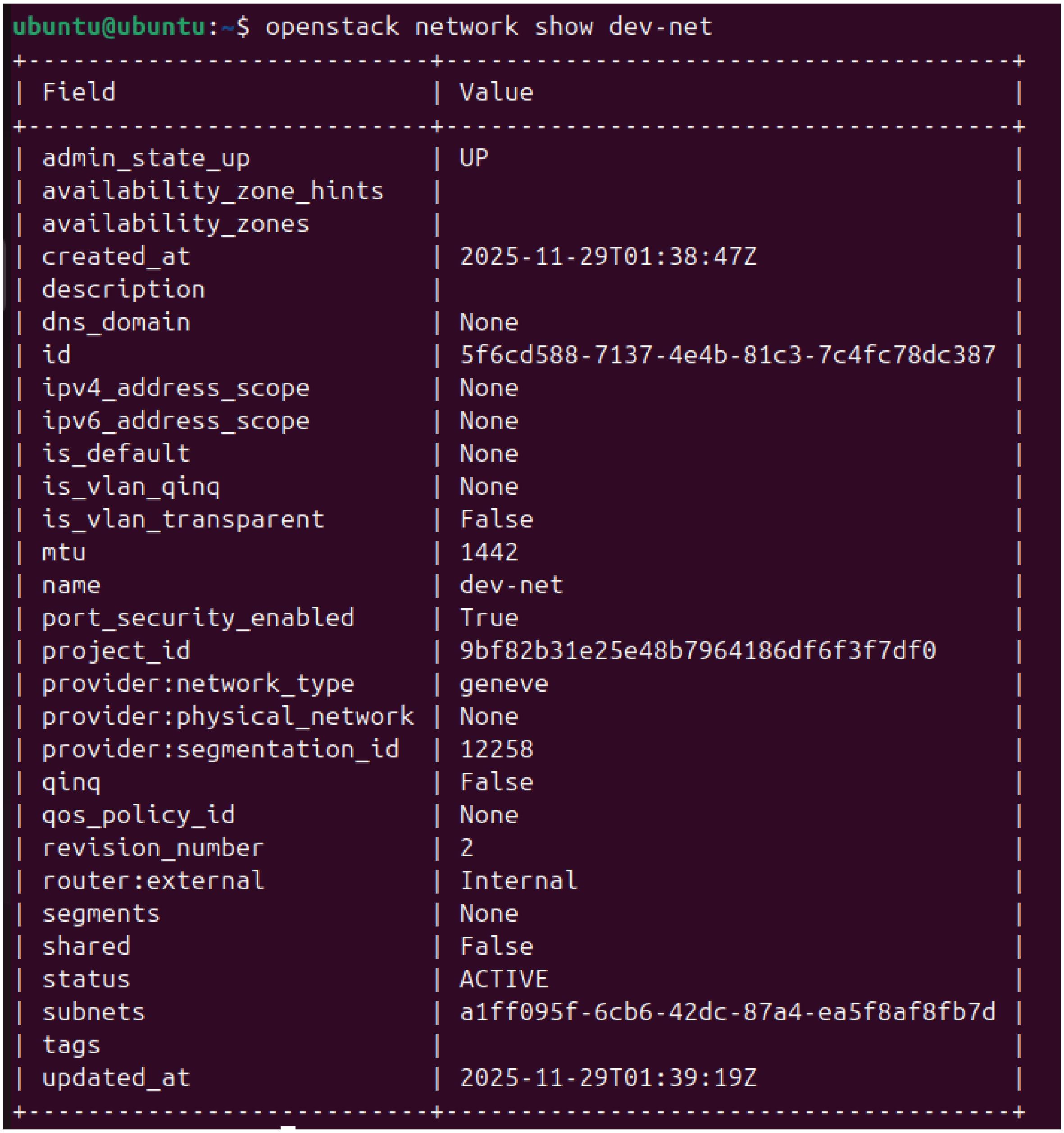
Step 11: Add a subnet to this network (CIDR example: 10.0.20.0/24):



```
ubuntu@ubuntu:~$ openstack subnet create --network dev-net --subnet-range 10.0.20.0/24 dev-subnet
+----------------------+--------------------------------------+
| Field                | Value                                |
+----------------------+--------------------------------------+
| allocation_pools     | 10.0.20.2-10.0.20.254                |
| cidr                 | 10.0.20.0/24                         |
| created_at           | 2025-11-29T01:39:19Z                 |
| description          |                                      |
| dns_nameservers      |                                      |
| dns_publish_fixed_ip | None                                 |
| enable_dhcp          | True                                 |
| gateway_ip           | 10.0.20.1                            |
| host_routes          |                                      |
| id                   | a1ff095f-6cb6-42dc-87a4-ea5f8af8fb7d |
| ip_version           | 4                                    |
| ipv6_address_mode    | None                                 |
| ipv6_ra_mode         | None                                 |
| name                 | dev-subnet                           |
| network_id           | 5f6cd588-7137-4e4b-81c3-7c4fc78dc387 |
| project_id           | 9bf82b31e25e48b7964186df6f3f7df0     |
| revision_number      | 0                                    |
| router:external      | False                                |
| segment_id           | None                                 |
| service_types        |                                      |
| subnetpool_id        | None                                 |
| tags                 |                                      |
| updated_at           | 2025-11-29T01:39:19Z                 |
+----------------------+--------------------------------------+
```

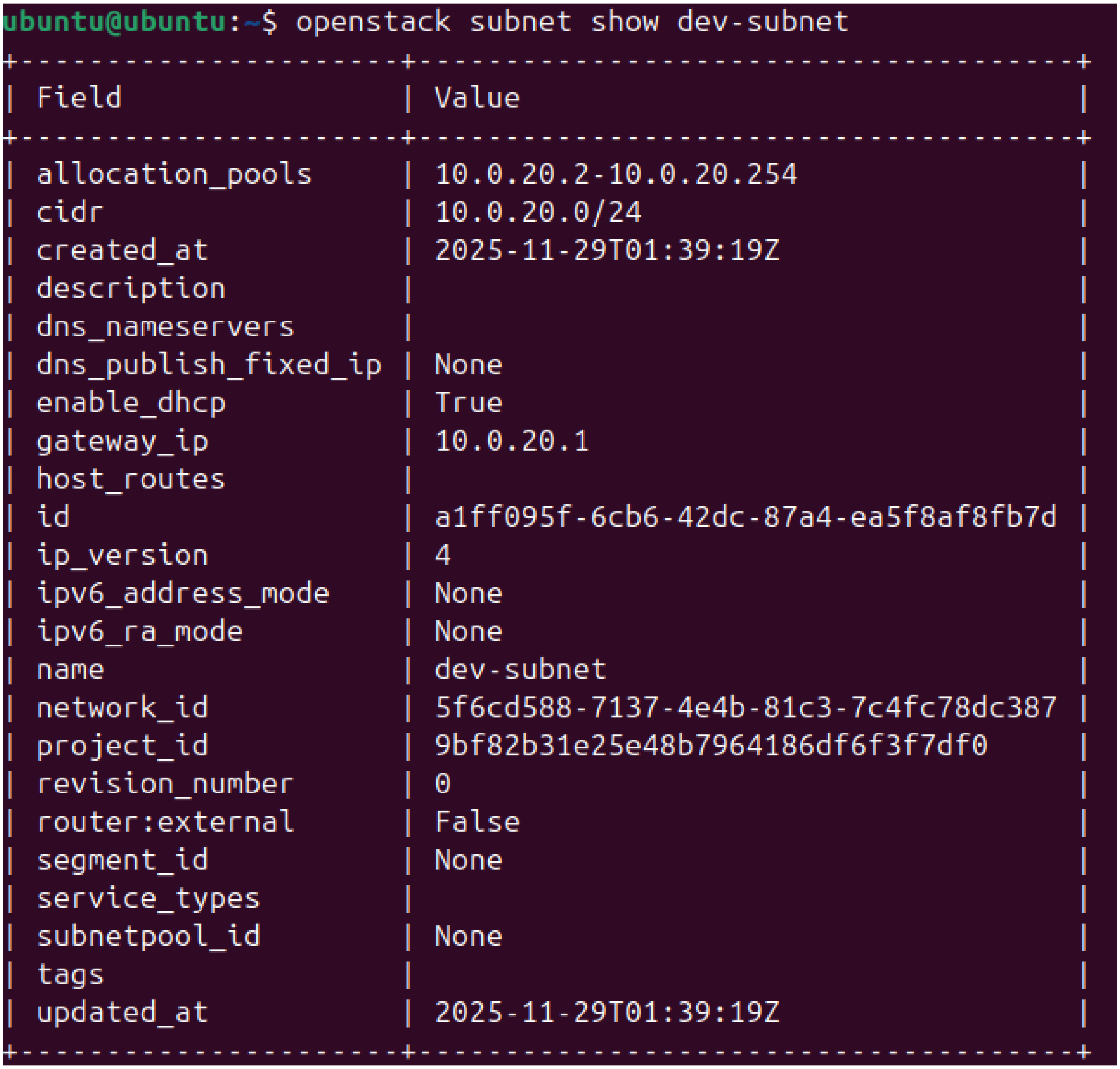
The subnet is now added to the dev-net network

Step 12: Review the network information



```
ubuntu@ubuntu:~$ openstack network show dev-net
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | UP                                   |
| availability_zone_hints   |                                      |
| availability_zones        |                                      |
| created_at                | 2025-11-29T01:38:47Z                 |
| description               |                                      |
| dns_domain                | None                                 |
| id                        | 5f6cd588-7137-4e4b-81c3-7c4fc78dc387 |
| ipv4_address_scope        | None                                 |
| ipv6_address_scope        | None                                 |
| is_default                | None                                 |
| is_vlan_qinq              | None                                 |
| is_vlan_transparent       | False                                |
| mtu                       | 1442                                 |
| name                      | dev-net                              |
| port_security_enabled     | True                                 |
| project_id                | 9bf82b31e25e48b7964186df6f3f7df0     |
| provider:network_type     | geneve                               |
| provider:physical_network | None                                 |
| provider:segmentation_id  | 12258                                |
| qinq                      | False                                |
| qos_policy_id             | None                                 |
| revision_number           | 2                                    |
| router:external           | Internal                             |
| segments                  | None                                 |
| shared                    | False                                |
| status                    | ACTIVE                               |
| subnets                   | a1ff095f-6cb6-42dc-87a4-ea5f8af8fb7d |
| tags                      |                                      |
| updated_at                | 2025-11-29T01:39:19Z                 |
+---------------------------+--------------------------------------+
```

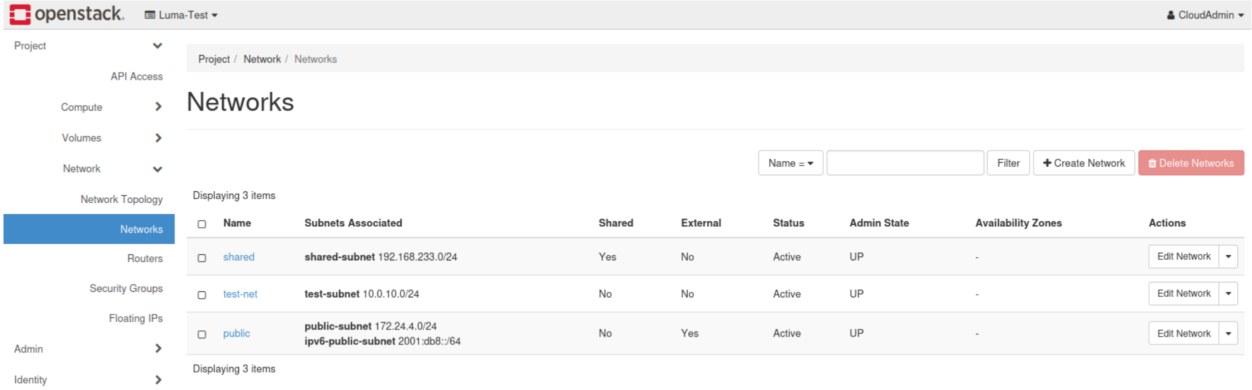
This network is not shared



```
ubuntu@ubuntu:~$ openstack subnet show dev-subnet
+----------------------+--------------------------------------+
| Field                | Value                                |
+----------------------+--------------------------------------+
| allocation_pools     | 10.0.20.2-10.0.20.254                |
| cidr                 | 10.0.20.0/24                         |
| created_at           | 2025-11-29T01:39:19Z                 |
| description          |                                      |
| dns_nameservers      |                                      |
| dns_publish_fixed_ip | None                                 |
| enable_dhcp          | True                                 |
| gateway_ip           | 10.0.20.1                            |
| host_routes          |                                      |
| id                   | a1ff095f-6cb6-42dc-87a4-ea5f8af8fb7d |
| ip_version           | 4                                    |
| ipv6_address_mode    | None                                 |
| ipv6_ra_mode         | None                                 |
| name                 | dev-subnet                           |
| network_id           | 5f6cd588-7137-4e4b-81c3-7c4fc78dc387 |
| project_id           | 9bf82b31e25e48b7964186df6f3f7df0     |
| revision_number      | 0                                    |
| router:external      | False                                |
| segment_id           | None                                 |
| service_types        |                                      |
| subnetpool_id        | None                                 |
| tags                 |                                      |
| updated_at           | 2025-11-29T01:39:19Z                 |
+----------------------+--------------------------------------+
```

The subnet matches the expected range

Step 13: Ensure that this network is restricted to the Dev project:



Networks

Displaying 3 items

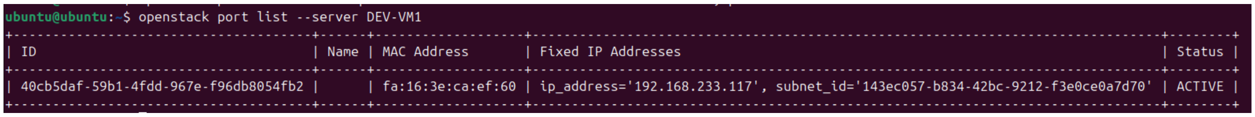
□	Name	Subnets Associated	Shared	External	Status	Admin State	Availability Zones	Actions
□	shared	**shared-subnet** 192.168.233.0/24	Yes	No	Active	UP	-	Edit Network
□	test-net	**test-subnet** 10.0.10.0/24	No	No	Active	UP	-	Edit Network
□	public	**public-subnet** 172.24.4.0/24 **ipv6-public-subnet** 2001:db8::/64	No	Yes	Active	UP	-	Edit Network

Displaying 3 items

The Test environment cannot see "dev-net" [3]

1.4 Migrating the Dev VM to the Dev Network

Step 14: List current ports for the Dev VM by typing "openstack port list --server DEV-VM1" in the terminal:



```
ubuntu@ubuntu:~$ openstack port list --server DEV-VM1
+--------------------------------------+------+-------------------+---------------------------------------------------------------------------------+--------+
| ID                                   | Name | MAC Address       | Fixed IP Addresses                                                              | Status |
+--------------------------------------+------+-------------------+---------------------------------------------------------------------------------+--------+
| 40cb5daf-59b1-4fdd-967e-f96db8054fb2 |      | fa:16:3e:ca:ef:60 | ip_address='192.168.233.117', subnet_id='143ec057-b834-42bc-9212-f3e0ce0a7d70' | ACTIVE |
+--------------------------------------+------+-------------------+---------------------------------------------------------------------------------+--------+
```

The current IP is 192.168.233.117 and you can see we are on the "shared" network

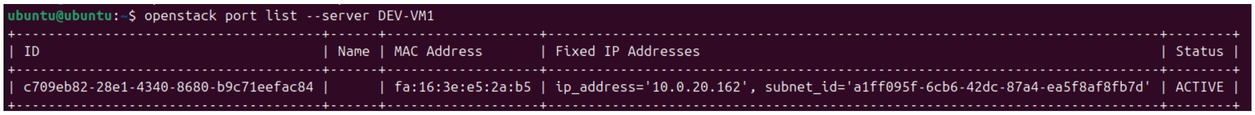
Step 15: Detach it from the provider network by typing "openstack server remove network DEV-VM1 provider" into the terminal.

(no output is displayed)

Step 16: Attach it to the new Dev network by typing "openstack server add network DEV-VM1 dev-net" into the terminal.

(no output is displayed)

Step 17: Verify attachment and assigned IP by typing “openstack port list --server DEV-VM1" into the terminal to confirm the VM now resides solely on dev-subnet:

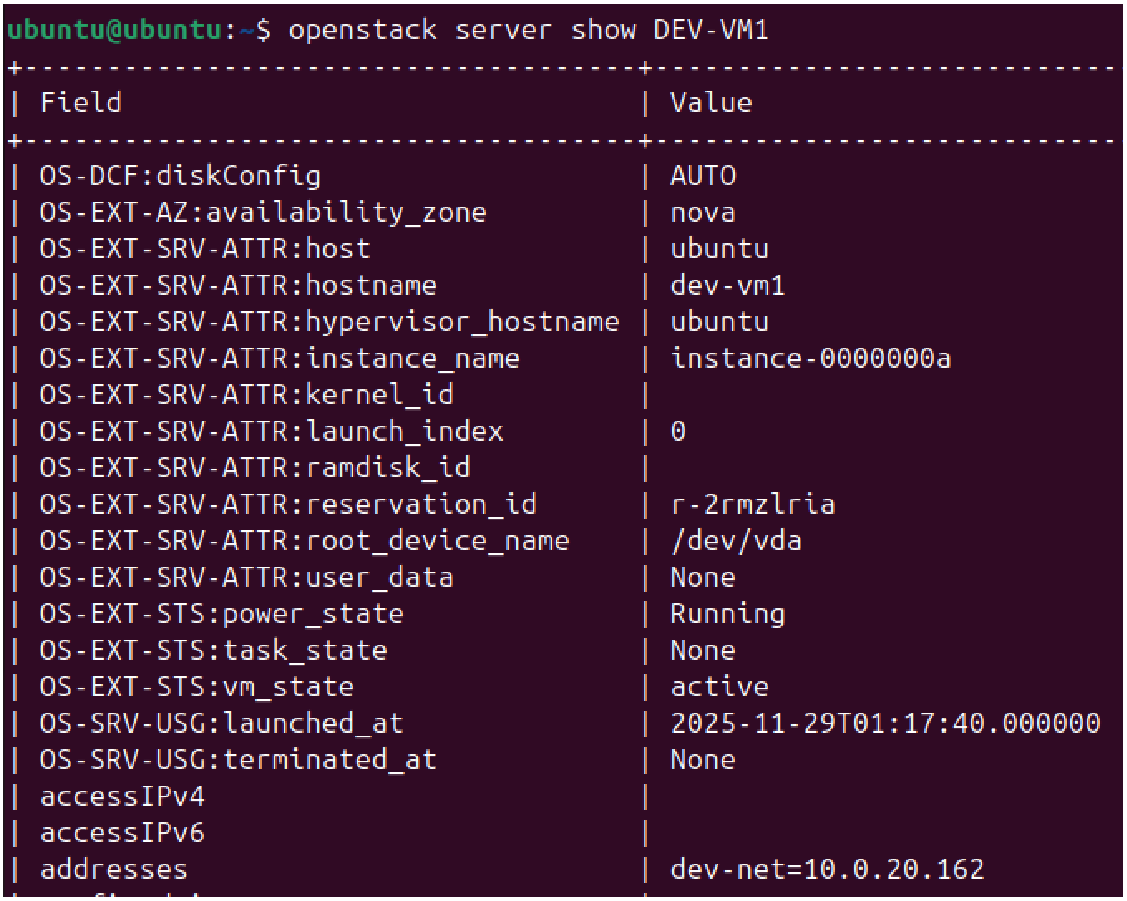


```
ubuntu@ubuntu:~$ openstack port list --server DEV-VM1
+--------------------------------------+------+-------------------+-----------------------------------------------------------------------------+--------+
| ID                                   | Name | MAC Address       | Fixed IP Addresses                                                          | Status |
+--------------------------------------+------+-------------------+-----------------------------------------------------------------------------+--------+
| c709eb82-28e1-4340-8680-b9c71eefac84 |      | fa:16:3e:e5:2a:b5 | ip_address='10.0.20.162', subnet_id='a1ff095f-6cb6-42dc-87a4-ea5f8af8fb7d' | ACTIVE |
+--------------------------------------+------+-------------------+-----------------------------------------------------------------------------+--------+
```

The IP has now changed to 10.0.20.162. Your instance may vary but take note of your IP

1.5 Validating Isolation Between Dev and Test Networks

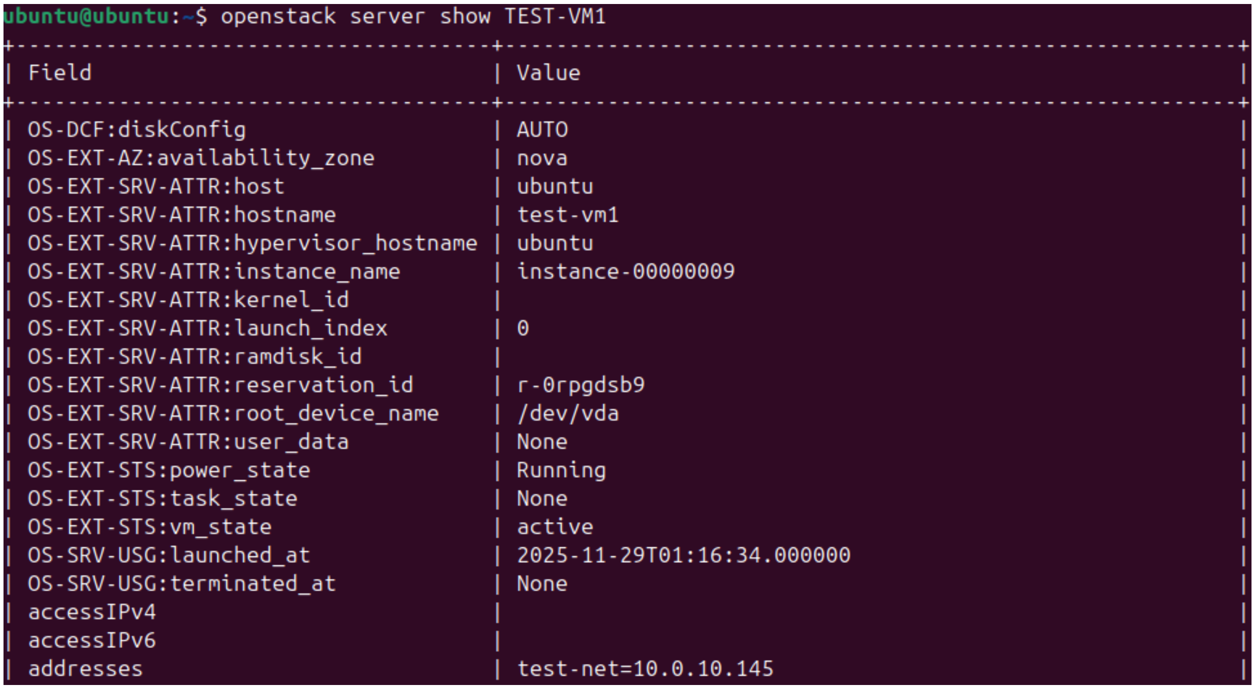
Step 18: Retrieve both VMs’ new internal IPs:



```
ubuntu@ubuntu:~$ openstack server show DEV-VM1
+-------------------------------------+---------------------------
| Field                               | Value
+-------------------------------------+---------------------------
| OS-DCF:diskConfig                   | AUTO
| OS-EXT-AZ:availability_zone         | nova
| OS-EXT-SRV-ATTR:host                | ubuntu
| OS-EXT-SRV-ATTR:hostname            | dev-vm1
| OS-EXT-SRV-ATTR:hypervisor_hostname | ubuntu
| OS-EXT-SRV-ATTR:instance_name       | instance-0000000a
| OS-EXT-SRV-ATTR:kernel_id           |
| OS-EXT-SRV-ATTR:launch_index        | 0
| OS-EXT-SRV-ATTR:ramdisk_id          |
| OS-EXT-SRV-ATTR:reservation_id      | r-2rmzlria
| OS-EXT-SRV-ATTR:root_device_name    | /dev/vda
| OS-EXT-SRV-ATTR:user_data           | None
| OS-EXT-STS:power_state              | Running
| OS-EXT-STS:task_state               | None
| OS-EXT-STS:vm_state                 | active
| OS-SRV-USG:launched_at              | 2025-11-29T01:17:40.000000
| OS-SRV-USG:terminated_at            | None
| accessIPv4                          |
| accessIPv6                          |
| addresses                           | dev-net=10.0.20.162
```

Notice that we are on the dev-net

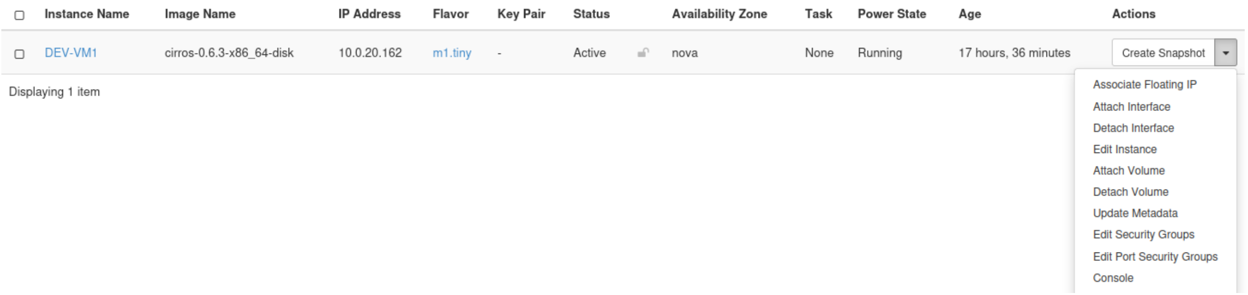
Step 19: Source the Luma-Test-openrc.sh file and view the new IP for TEST-VM1:



```
ubuntu@ubuntu:~$ openstack server show TEST-VM1
+-------------------------------------+-------------------------------------------------------+
| Field                               | Value                                                 |
+-------------------------------------+-------------------------------------------------------+
| OS-DCF:diskConfig                   | AUTO                                                  |
| OS-EXT-AZ:availability_zone         | nova                                                  |
| OS-EXT-SRV-ATTR:host                | ubuntu                                                |
| OS-EXT-SRV-ATTR:hostname            | test-vm1                                              |
| OS-EXT-SRV-ATTR:hypervisor_hostname | ubuntu                                                |
| OS-EXT-SRV-ATTR:instance_name       | instance-00000009                                     |
| OS-EXT-SRV-ATTR:kernel_id           |                                                       |
| OS-EXT-SRV-ATTR:launch_index        | 0                                                     |
| OS-EXT-SRV-ATTR:ramdisk_id          |                                                       |
| OS-EXT-SRV-ATTR:reservation_id      | r-0rpgdsb9                                            |
| OS-EXT-SRV-ATTR:root_device_name    | /dev/vda                                              |
| OS-EXT-SRV-ATTR:user_data           | None                                                  |
| OS-EXT-STS:power_state              | Running                                               |
| OS-EXT-STS:task_state               | None                                                  |
| OS-EXT-STS:vm_state                 | active                                                |
| OS-SRV-USG:launched_at              | 2025-11-29T01:16:34.000000                            |
| OS-SRV-USG:terminated_at            | None                                                  |
| accessIPv4                          |                                                       |
| accessIPv6                          |                                                       |
| addresses                           | test-net=10.0.10.145                                  |
```

Notice that we are on the Test-Net

Step 20: Attempt cross-project pings by logging in to your instance in horizon and selecting “Console” from the drop down of your VM under Compute -> Instances:

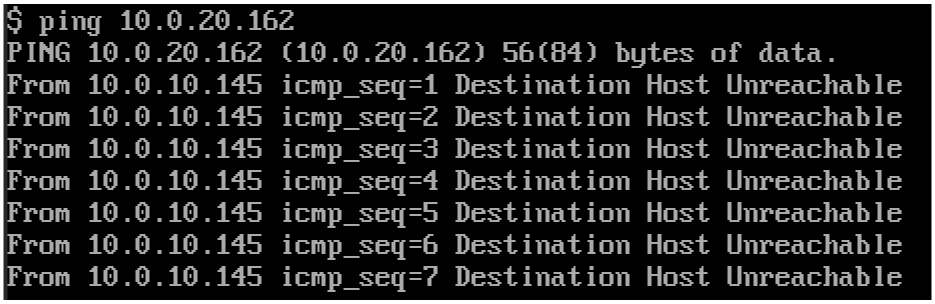


□	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
□	DEV-VM1	cirros-0.6.3-x86_64-disk	10.0.20.162	m1.tiny	-	Active	nova	None	Running	17 hours, 36 minutes	Create Snapshot ▾

Displaying 1 item

The username and password will come up on the next screen. Login and continue

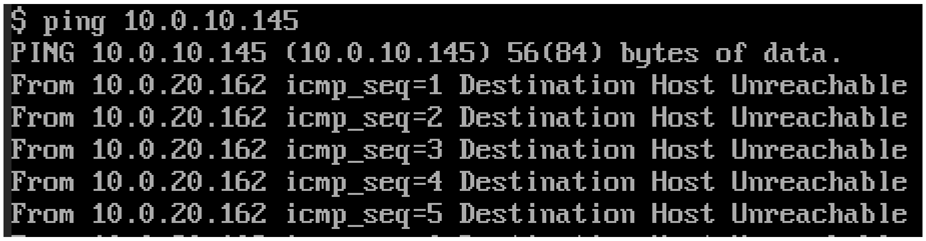
Step 21: From the Test VM console ping 10.0.20.162:



```
$ ping 10.0.20.162
PING 10.0.20.162 (10.0.20.162) 56(84) bytes of data.
From 10.0.10.145 icmp_seq=1 Destination Host Unreachable
From 10.0.10.145 icmp_seq=2 Destination Host Unreachable
From 10.0.10.145 icmp_seq=3 Destination Host Unreachable
From 10.0.10.145 icmp_seq=4 Destination Host Unreachable
From 10.0.10.145 icmp_seq=5 Destination Host Unreachable
From 10.0.10.145 icmp_seq=6 Destination Host Unreachable
From 10.0.10.145 icmp_seq=7 Destination Host Unreachable
```

Ping does not work due to separate networks with no routers [3][5]

Step 22: From the Dev VM console ping 10.0.10.145:



```
$ ping 10.0.10.145
PING 10.0.10.145 (10.0.10.145) 56(84) bytes of data.
From 10.0.20.162 icmp_seq=1 Destination Host Unreachable
From 10.0.20.162 icmp_seq=2 Destination Host Unreachable
From 10.0.20.162 icmp_seq=3 Destination Host Unreachable
From 10.0.20.162 icmp_seq=4 Destination Host Unreachable
From 10.0.20.162 icmp_seq=5 Destination Host Unreachable
```

Ping does not work due to separate networks with no routers

Step 23: Observe that neither VM can reach the other, confirming that the networks are isolated at Layer 2/3.

1.6 Section Summary

Document the segmentation results:

- Test and Dev now operate on separate, project-owned networks.
- Instances can no longer communicate across project boundaries. [3]
- Default security groups remain permissive, but isolation is enforced by network segmentation alone.
- This segmentation prepares the environment for Section 2, where fine-grained security rules will be implemented.

Section 2: Defining Security Boundaries Through Rule Sets

With the network segments in place, our next deliverable involves tightening LumaTech's control points using tailored security group rules. [7] Here, we refine how each instance can send or receive traffic, defining explicit rule sets that mirror the company's operational requirements while minimizing unnecessary exposure. This section demonstrates how structured rule enforcement strengthens the segmentation created earlier, giving LumaTech more predictable and auditable communication flows across its cloud resources.

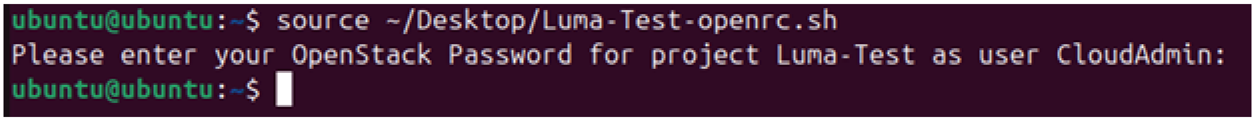
****Disclaimer**** TEST-VM1 & DEV-VM1 were changed to TEST-VM-NEW & DEV-VM-NEW due to operational complications with shared VM instances.

2.1 Reviewing the Default Security Group in Each Project

Step 1: Start with the Test project credentials:

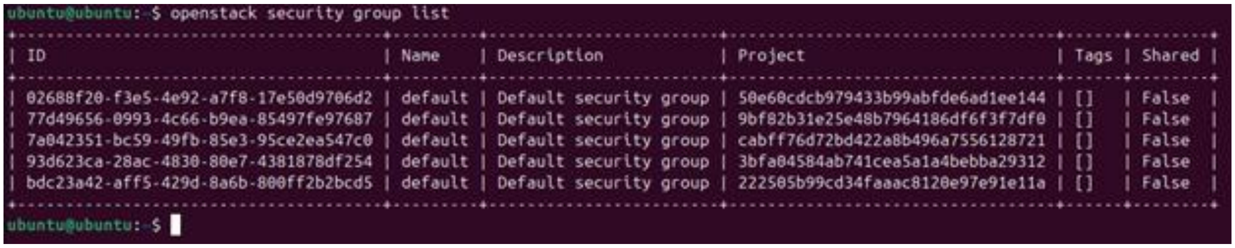
Username: CloudAdmin

Password: password



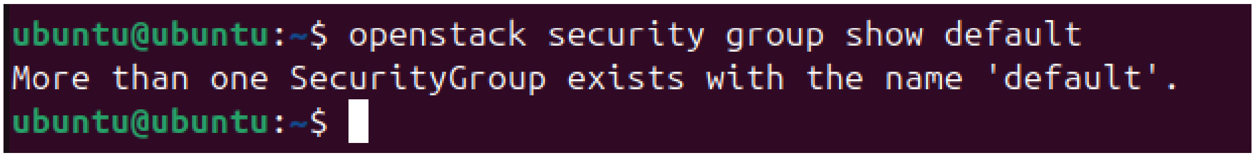
```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Test-openrc.sh
Please enter your OpenStack Password for project Luma-Test as user CloudAdmin:
ubuntu@ubuntu:~$ 
```

Step 2: List available security groups by typing "openstack security group list" into the terminal:



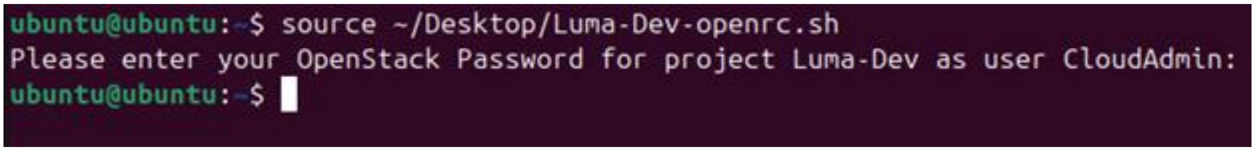
```
ubuntu@ubuntu:~$ openstack security group list
+--------------------------------------+---------+------------------------+----------------------------------+------+--------+
| ID                                   | Name    | Description            | Project                          | Tags | Shared |
+--------------------------------------+---------+------------------------+----------------------------------+------+--------+
| 02688f20-f3e5-4e92-a7f8-17e50d9706d2 | default | Default security group | 50e60cdcb979433b99abfde6ad1ee144 | []   | False  |
| 77d49656-0993-4c66-b9ea-85497fe97687 | default | Default security group | 9bf82b31e25e48b7964186df6f3f7df0 | []   | False  |
| 7a042351-bc59-49fb-85e3-95ce2ea547c0 | default | Default security group | cabff76d72bd422a8b496a7556128721 | []   | False  |
| 93d623ca-28ac-4830-80e7-4381878df254 | default | Default security group | 3bfa04584ab741cea5a1a4bebba29312 | []   | False  |
| bdc23a42-aff5-429d-8a6b-800ff2b2bcd5 | default | Default security group | 222505b99cd34faaac8120e97e91e11a | []   | False  |
+--------------------------------------+---------+------------------------+----------------------------------+------+--------+
ubuntu@ubuntu:~$ 
```

Step 3: Inspect the default security group:

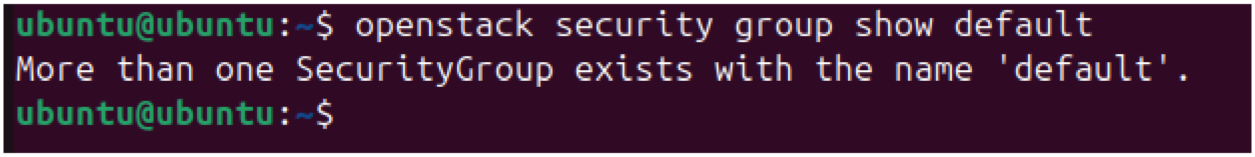


```
ubuntu@ubuntu:~$ openstack security group show default
More than one SecurityGroup exists with the name 'default'.
ubuntu@ubuntu:~$
```

Step 4: Repeat the same process for the Dev project:



```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Dev-openrc.sh
Please enter your OpenStack Password for project Luma-Dev as user CloudAdmin:
ubuntu@ubuntu:~$
```

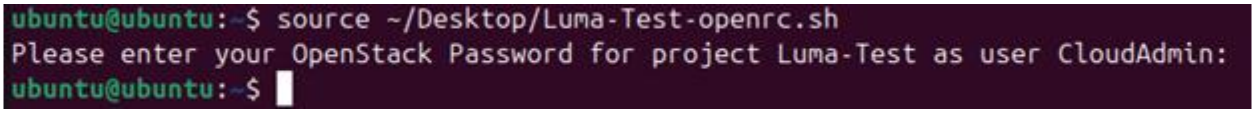


```
ubuntu@ubuntu:~$ openstack security group show default
More than one SecurityGroup exists with the name 'default'.
ubuntu@ubuntu:~$
```

Both projects rely on the same permissive default rules that allow broad communication. [7][5]

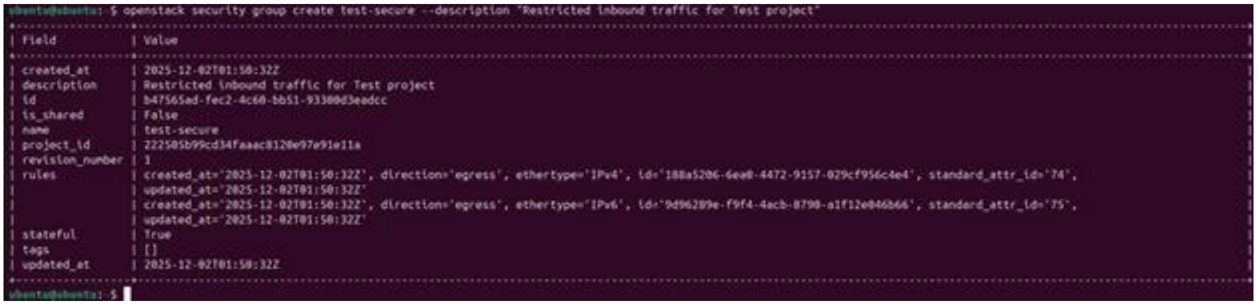
2.2 Creating a Restrictive Security Group for the Test Project

Step 5: Switch to the Test project:



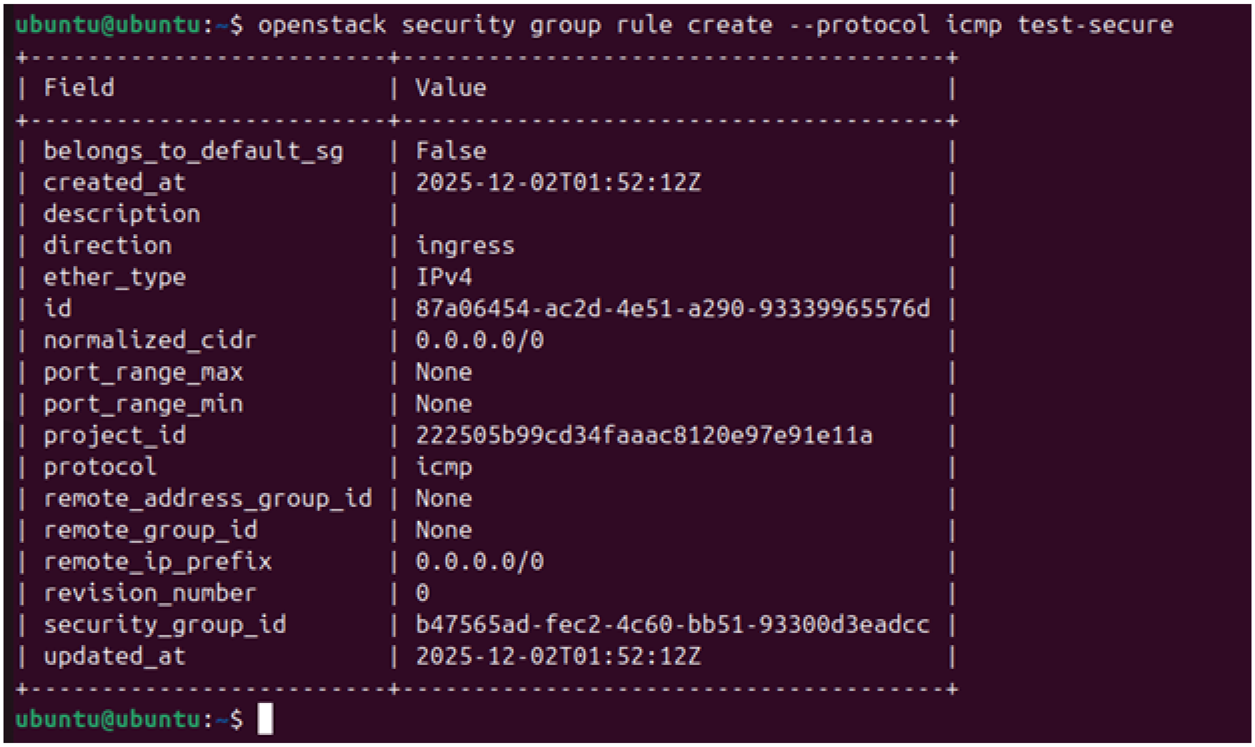
```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Test-openrc.sh
Please enter your OpenStack Password for project Luma-Test as user CloudAdmin:
ubuntu@ubuntu:~$
```

Step 6: Create a new security group called test-secure by typing “openstack security group create test-secure --description “Restricted inbound traffic for Test project”” into the terminal:



```
ubuntu@ubuntu:~$ openstack security group create test-secure --description "Restricted inbound traffic for Test project"
+-----------------+-------------------------------------------------------------------------------------------------------------------------------+
| Field           | Value                                                                                                                         |
+-----------------+-------------------------------------------------------------------------------------------------------------------------------+
| created_at      | 2025-12-02T01:50:32Z                                                                                                          |
| description     | Restricted inbound traffic for Test project                                                                                   |
| id              | b47565ad-fec2-4c60-bb51-93300d3eadcc                                                                                          |
| is_shared       | False                                                                                                                         |
| name            | test-secure                                                                                                                   |
| project_id      | 222505b99cd34faaac8120e97e91e11a                                                                                              |
| revision_number | 1                                                                                                                             |
| rules           | created_at='2025-12-02T01:50:32Z', direction='egress', ethertype='IPv4', id='188a5206-6ea0-4472-9157-029cf956c4e4', standard_attr_id='74', |
|                 | updated_at='2025-12-02T01:50:32Z'                                                                                             |
|                 | created_at='2025-12-02T01:50:32Z', direction='egress', ethertype='IPv6', id='9d96209e-f9f4-4acb-8790-a1f12e046b66', standard_attr_id='75', |
|                 | updated_at='2025-12-02T01:50:32Z'                                                                                             |
| stateful        | True                                                                                                                          |
| tags            | []                                                                                                                            |
| updated_at      | 2025-12-02T01:50:32Z                                                                                                          |
+-----------------+-------------------------------------------------------------------------------------------------------------------------------+
ubuntu@ubuntu:~$
```

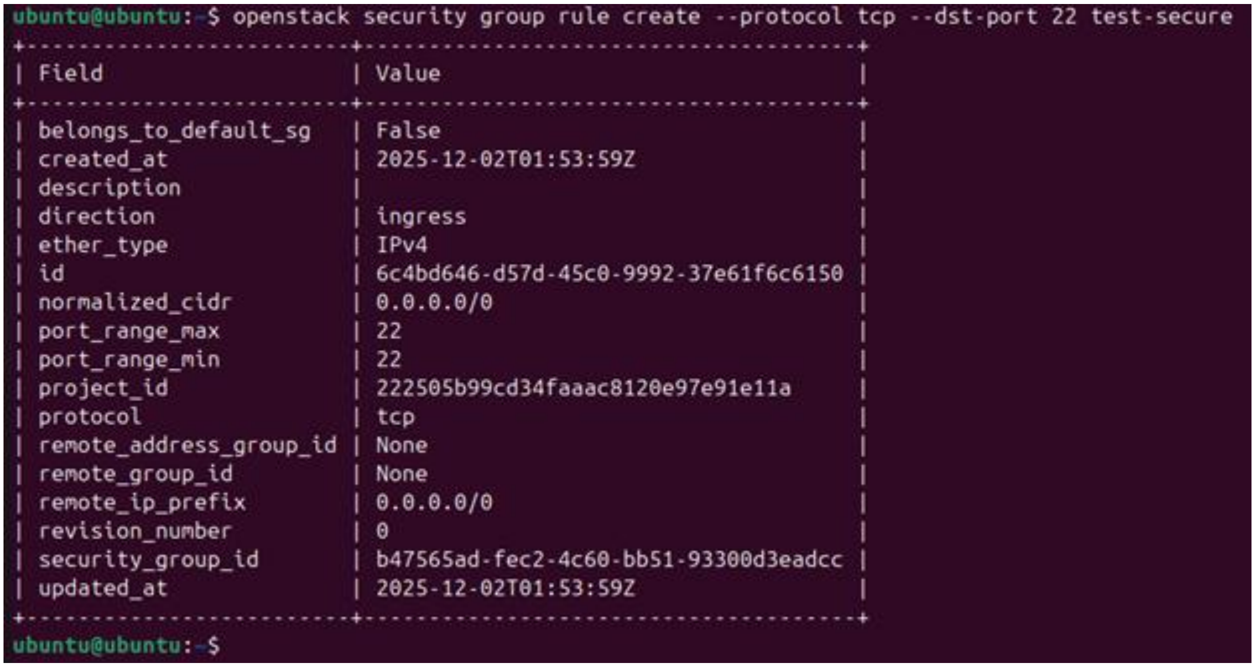
Step 7: Add an inbound ICMP rule:



```
ubuntu@ubuntu:~$ openstack security group rule create --protocol icmp test-secure
+-------------------------+--------------------------------------+
| Field                   | Value                                |
+-------------------------+--------------------------------------+
| belongs_to_default_sg   | False                                |
| created_at              | 2025-12-02T01:52:12Z                 |
| description             |                                      |
| direction               | ingress                              |
| ether_type              | IPv4                                 |
| id                      | 87a06454-ac2d-4e51-a290-93339965576d |
| normalized_cidr         | 0.0.0.0/0                            |
| port_range_max          | None                                 |
| port_range_min          | None                                 |
| project_id              | 222505b99cd34faaac8120e97e91e11a     |
| protocol                | icmp                                 |
| remote_address_group_id | None                                 |
| remote_group_id         | None                                 |
| remote_ip_prefix        | 0.0.0.0/0                            |
| revision_number         | 0                                    |
| security_group_id       | b47565ad-fec2-4c60-bb51-93300d3eadcc |
| updated_at              | 2025-12-02T01:52:12Z                 |
+-------------------------+--------------------------------------+
ubuntu@ubuntu:~$ 
```

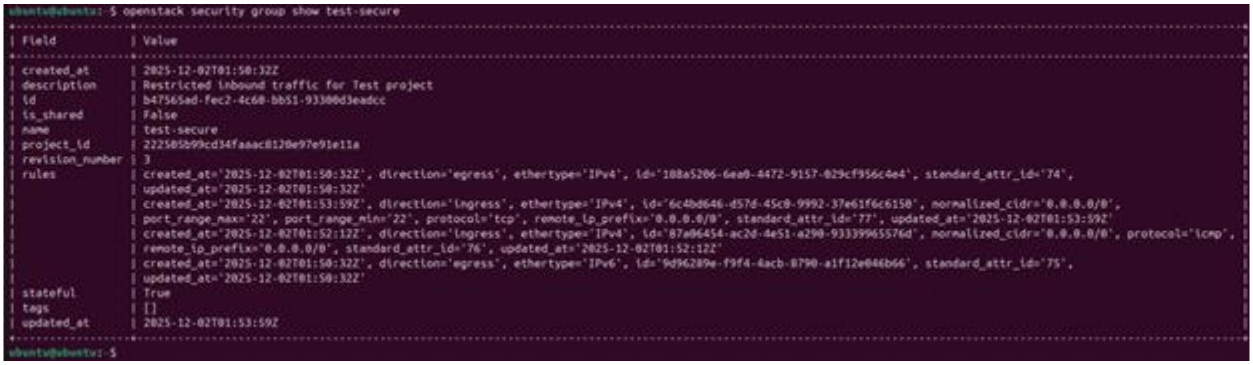
This will allow pings for testing purposes

Step 8: Add SSH access (port 22):



```
ubuntu@ubuntu:~$ openstack security group rule create --protocol tcp --dst-port 22 test-secure
+-------------------------+--------------------------------------+
| Field                   | Value                                |
+-------------------------+--------------------------------------+
| belongs_to_default_sg   | False                                |
| created_at              | 2025-12-02T01:53:59Z                 |
| description             |                                      |
| direction               | ingress                              |
| ether_type              | IPv4                                 |
| id                      | 6c4bd646-d57d-45c0-9992-37e61f6c6150 |
| normalized_cidr         | 0.0.0.0/0                            |
| port_range_max          | 22                                   |
| port_range_min          | 22                                   |
| project_id              | 222505b99cd34faaac8120e97e91e11a     |
| protocol                | tcp                                  |
| remote_address_group_id | None                                 |
| remote_group_id         | None                                 |
| remote_ip_prefix        | 0.0.0.0/0                            |
| revision_number         | 0                                    |
| security_group_id       | b47565ad-fec2-4c60-bb51-93300d3eadcc |
| updated_at              | 2025-12-02T01:53:59Z                 |
+-------------------------+--------------------------------------+
ubuntu@ubuntu:~$
```

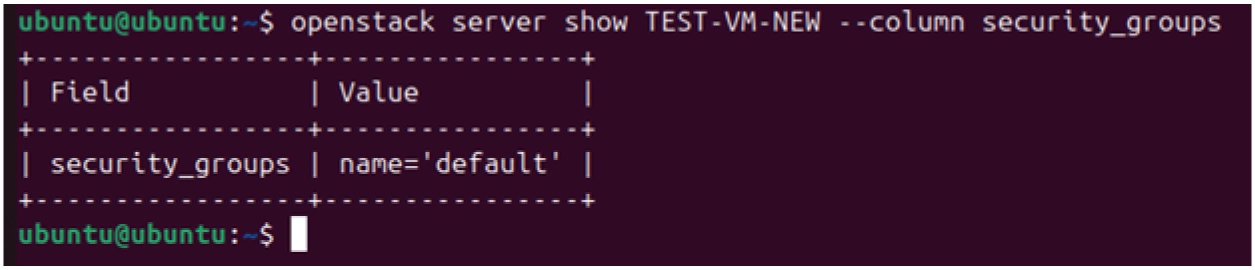
Step 9: Verify rules by typing “openstack security group show test-secure" into the terminal



```
ubuntu@ubuntu:~$ openstack security group show test-secure
+-----------------+--------------------------------------------------------------------------------------------------------------------------------------+
| Field           | Value                                                                                                                                |
+-----------------+--------------------------------------------------------------------------------------------------------------------------------------+
| created_at      | 2025-12-02T01:50:32Z                                                                                                                 |
| description     | Restricted inbound traffic for Test project                                                                                          |
| id              | b47565ad-fec2-4c60-bb51-93300d3eadcc                                                                                                 |
| is_shared       | False                                                                                                                                |
| name            | test-secure                                                                                                                          |
| project_id      | 222505b99cd34faaac8120e97e91e11a                                                                                                     |
| revision_number | 3                                                                                                                                    |
| rules           | created_at='2025-12-02T01:50:32Z', direction='egress', ethertype='IPv4', id='188a5206-6ea0-4472-9157-029cf956c4e4', standard_attr_id='74',          |
|                 | updated_at='2025-12-02T01:50:32Z'                                                                                                    |
|                 | created_at='2025-12-02T01:53:59Z', direction='ingress', ethertype='IPv4', id='6c4bd646-d57d-45c0-9992-37e61f6c6150', normalized_cidr='0.0.0.0/0',  |
|                 | port_range_max='22', port_range_min='22', protocol='tcp', remote_ip_prefix='0.0.0.0/0', standard_attr_id='77', updated_at='2025-12-02T01:53:59Z'   |
|                 | created_at='2025-12-02T01:52:12Z', direction='ingress', ethertype='IPv4', id='87a06454-ac2d-4e51-a290-93339965576d', normalized_cidr='0.0.0.0/0', protocol='icmp', |
|                 | remote_ip_prefix='0.0.0.0/0', standard_attr_id='76', updated_at='2025-12-02T01:52:12Z'                                               |
|                 | created_at='2025-12-02T01:50:32Z', direction='egress', ethertype='IPv6', id='9d96289e-f9f4-4acb-8790-a1f12e046b66', standard_attr_id='75',          |
|                 | updated_at='2025-12-02T01:50:32Z'                                                                                                    |
| stateful        | True                                                                                                                                 |
| tags            | []                                                                                                                                   |
| updated_at      | 2025-12-02T01:53:59Z                                                                                                                 |
+-----------------+--------------------------------------------------------------------------------------------------------------------------------------+
ubuntu@ubuntu:~$
```

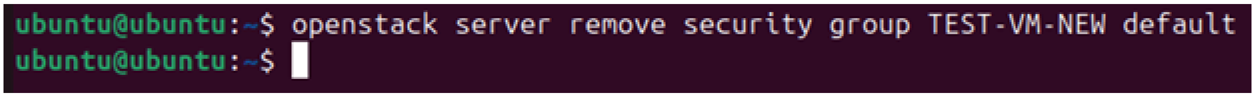
2.3 Assigning the New Security Group to the Test VM

Step 10: List the VM’s security groups:



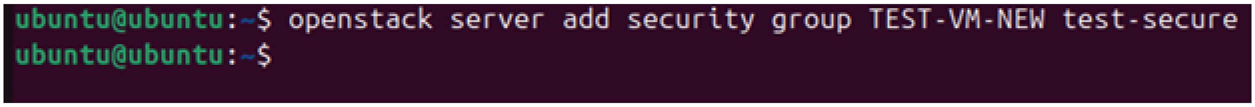
```
ubuntu@ubuntu:~$ openstack server show TEST-VM-NEW --column security_groups
+-----------------+----------------+
| Field           | Value          |
+-----------------+----------------+
| security_groups | name='default' |
+-----------------+----------------+
ubuntu@ubuntu:~$
```

Step 11: Remove the default group:



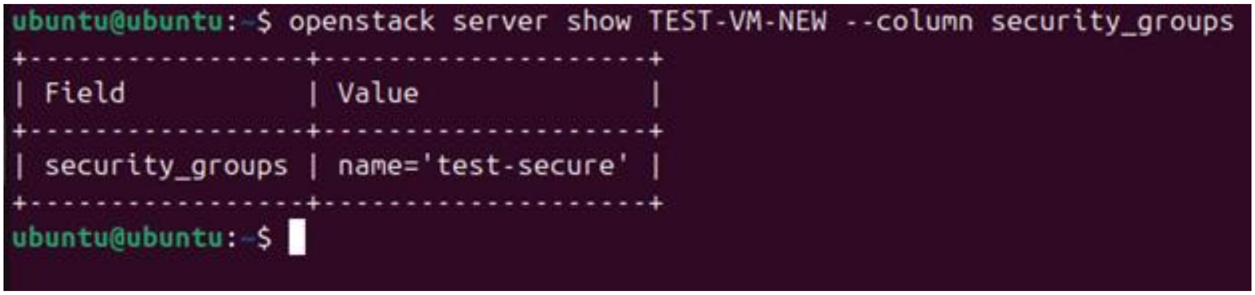
```
ubuntu@ubuntu:~$ openstack server remove security group TEST-VM-NEW default
ubuntu@ubuntu:~$
```

Step 12: Add the new group:



```
ubuntu@ubuntu:~$ openstack server add security group TEST-VM-NEW test-secure
ubuntu@ubuntu:~$
```

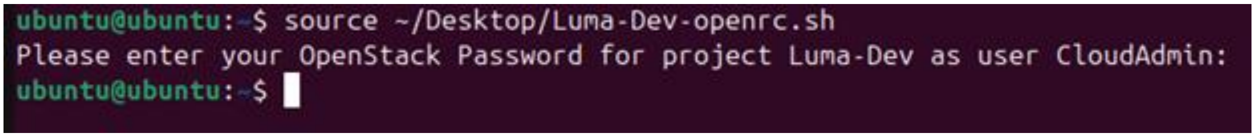
Step 13: Confirm the update:



```
ubuntu@ubuntu:~$ openstack server show TEST-VM-NEW --column security_groups
+-----------------+-------------------+
| Field           | Value             |
+-----------------+-------------------+
| security_groups | name='test-secure' |
+-----------------+-------------------+
ubuntu@ubuntu:~$
```

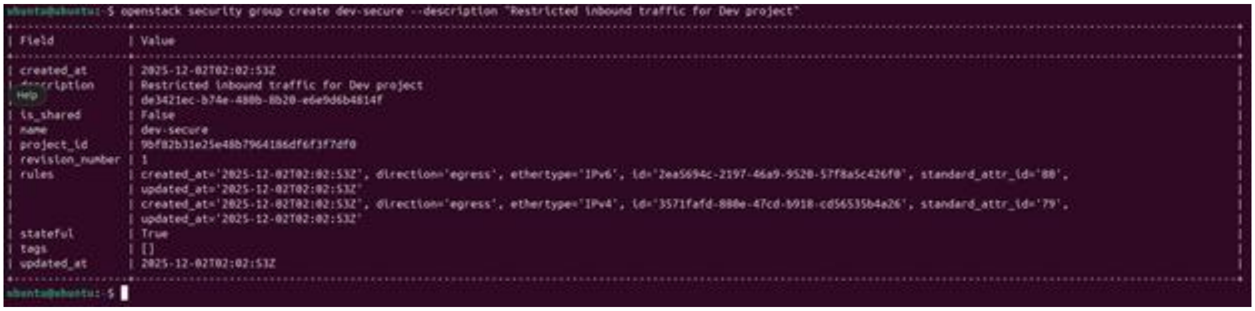
2.4 Creating a Restricted Security Group for the Dev Project

Step 14: Switch to Dev:



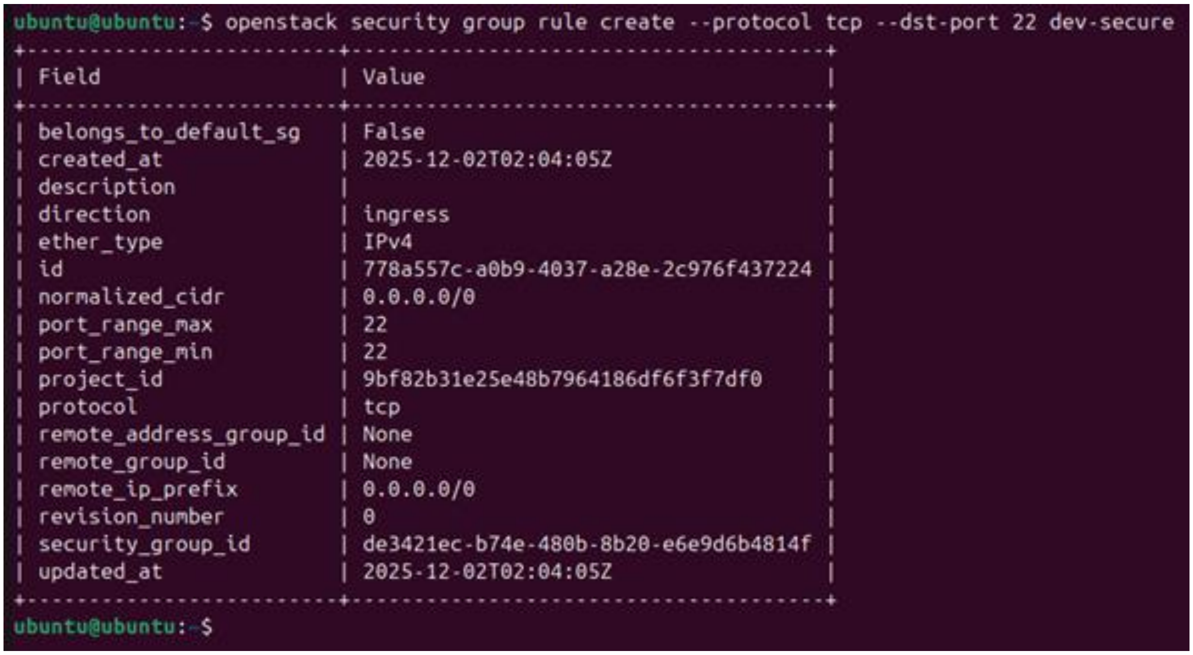
```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Dev-openrc.sh
Please enter your OpenStack Password for project Luma-Dev as user CloudAdmin:
ubuntu@ubuntu:~$
```

Step 15: Create the dev-secure group by typing “openstack security group create dev-secure --description “Restricted inbound traffic for Dev project”” into the terminal:



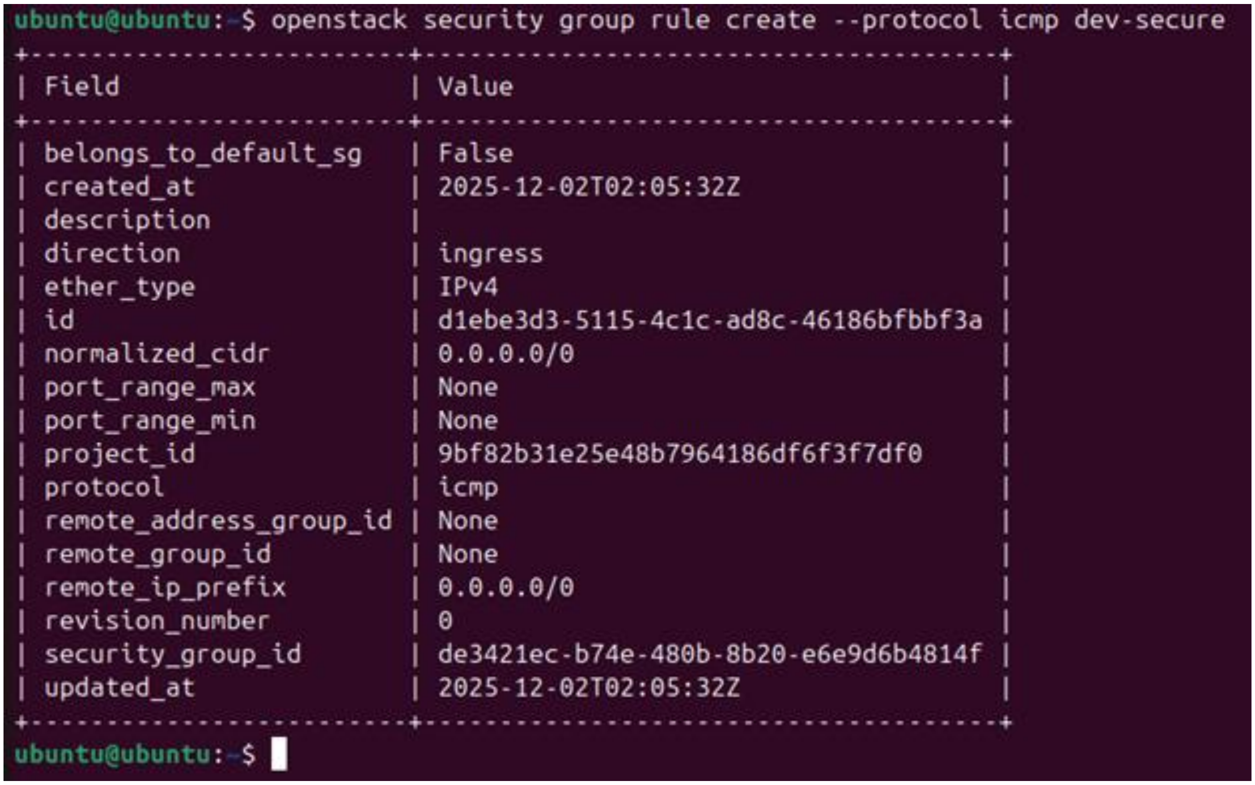
```
ubuntu@ubuntu:~$ openstack security group create dev-secure --description "Restricted inbound traffic for Dev project"
+-----------------+--------------------------------------------------------------------------------------------------------------------------------------------+
| Field           | Value                                                                                                                                      |
+-----------------+--------------------------------------------------------------------------------------------------------------------------------------------+
| created_at      | 2025-12-02T02:02:53Z                                                                                                                       |
| description     | Restricted inbound traffic for Dev project                                                                                                 |
|                 | de3421ec-b74e-480b-8b20-e6e9d6b4814f                                                                                                       |
| is_shared       | False                                                                                                                                      |
| name            | dev-secure                                                                                                                                 |
| project_id      | 9bf82b31e25e48b7964186df6f3f7df0                                                                                                           |
| revision_number | 1                                                                                                                                          |
| rules           | created_at='2025-12-02T02:02:53Z', direction='egress', ethertype='IPv6', id='2ea5694c-2197-46a9-9520-57f8a5c426f0', standard_attr_id='80', |
|                 | updated_at='2025-12-02T02:02:53Z'                                                                                                          |
|                 | created_at='2025-12-02T02:02:53Z', direction='egress', ethertype='IPv4', id='3571fafd-880e-47cd-b918-cd56535b4a26', standard_attr_id='79', |
|                 | updated_at='2025-12-02T02:02:53Z'                                                                                                          |
| stateful        | True                                                                                                                                       |
| tags            | []                                                                                                                                         |
| updated_at      | 2025-12-02T02:02:53Z                                                                                                                       |
+-----------------+--------------------------------------------------------------------------------------------------------------------------------------------+
ubuntu@ubuntu:~$
```

Step 16: Add SSH access for administrative control:



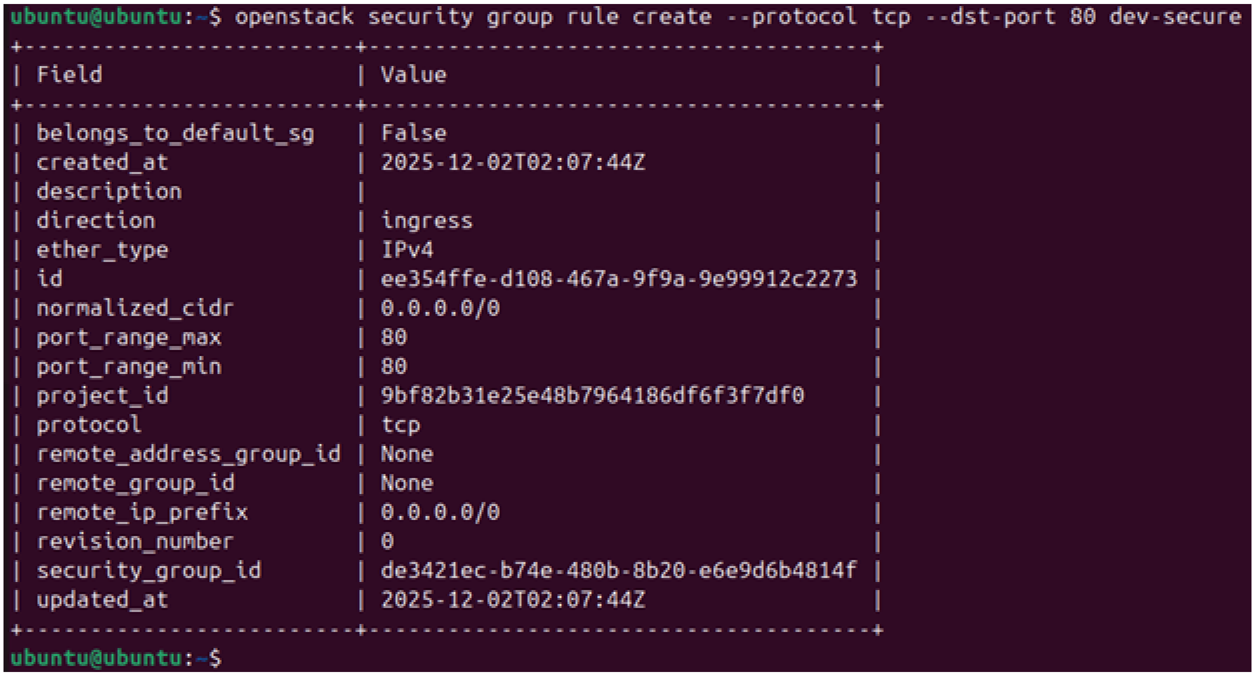
```
ubuntu@ubuntu:~$ openstack security group rule create --protocol tcp --dst-port 22 dev-secure
+-------------------------+--------------------------------------+
| Field                   | Value                                |
+-------------------------+--------------------------------------+
| belongs_to_default_sg   | False                                |
| created_at              | 2025-12-02T02:04:05Z                 |
| description             |                                      |
| direction               | ingress                              |
| ether_type              | IPv4                                 |
| id                      | 778a557c-a0b9-4037-a28e-2c976f437224 |
| normalized_cidr         | 0.0.0.0/0                            |
| port_range_max          | 22                                   |
| port_range_min          | 22                                   |
| project_id              | 9bf82b31e25e48b7964186df6f3f7df0     |
| protocol                | tcp                                  |
| remote_address_group_id | None                                 |
| remote_group_id         | None                                 |
| remote_ip_prefix        | 0.0.0.0/0                            |
| revision_number         | 0                                    |
| security_group_id       | de3421ec-b74e-480b-8b20-e6e9d6b4814f |
| updated_at              | 2025-12-02T02:04:05Z                 |
+-------------------------+--------------------------------------+
ubuntu@ubuntu:~$
```

Step 17: Add ICMP for connectivity tests:



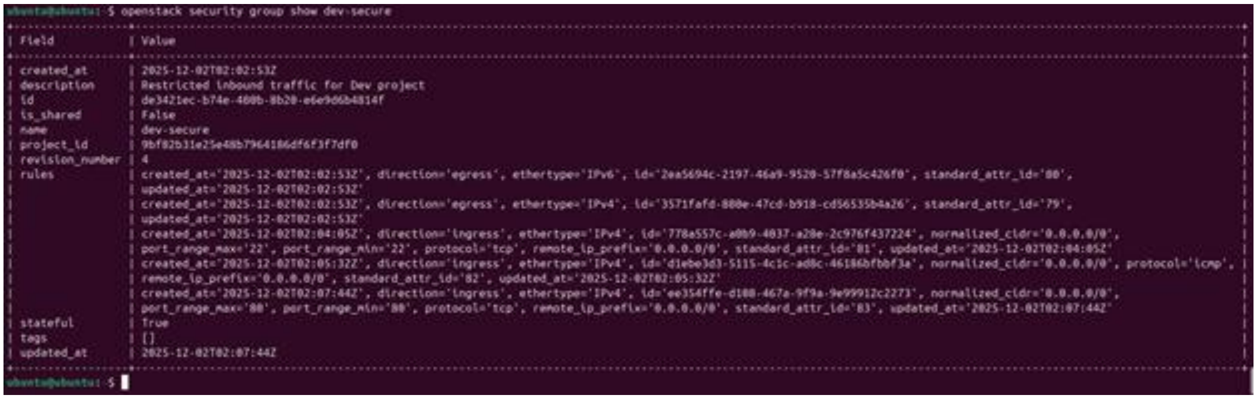
```
ubuntu@ubuntu:~$ openstack security group rule create --protocol icmp dev-secure
+-------------------------+--------------------------------------+
| Field                   | Value                                |
+-------------------------+--------------------------------------+
| belongs_to_default_sg   | False                                |
| created_at              | 2025-12-02T02:05:32Z                 |
| description             |                                      |
| direction               | ingress                              |
| ether_type              | IPv4                                 |
| id                      | d1ebe3d3-5115-4c1c-ad8c-46186bfbbf3a |
| normalized_cidr         | 0.0.0.0/0                            |
| port_range_max          | None                                 |
| port_range_min          | None                                 |
| project_id              | 9bf82b31e25e48b7964186df6f3f7df0     |
| protocol                | icmp                                 |
| remote_address_group_id | None                                 |
| remote_group_id         | None                                 |
| remote_ip_prefix        | 0.0.0.0/0                            |
| revision_number         | 0                                    |
| security_group_id       | de3421ec-b74e-480b-8b20-e6e9d6b4814f |
| updated_at              | 2025-12-02T02:05:32Z                 |
+-------------------------+--------------------------------------+
ubuntu@ubuntu:~$
```

Step 18: Add HTTP access for web services:



```
ubuntu@ubuntu:~$ openstack security group rule create --protocol tcp --dst-port 80 dev-secure
+-------------------------+--------------------------------------+
| Field                   | Value                                |
+-------------------------+--------------------------------------+
| belongs_to_default_sg   | False                                |
| created_at              | 2025-12-02T02:07:44Z                 |
| description             |                                      |
| direction               | ingress                              |
| ether_type              | IPv4                                 |
| id                      | ee354ffe-d108-467a-9f9a-9e99912c2273 |
| normalized_cidr         | 0.0.0.0/0                            |
| port_range_max          | 80                                   |
| port_range_min          | 80                                   |
| project_id              | 9bf82b31e25e48b7964186df6f3f7df0     |
| protocol                | tcp                                  |
| remote_address_group_id | None                                 |
| remote_group_id         | None                                 |
| remote_ip_prefix        | 0.0.0.0/0                            |
| revision_number         | 0                                    |
| security_group_id       | de3421ec-b74e-480b-8b20-e6e9d6b4814f |
| updated_at              | 2025-12-02T02:07:44Z                 |
+-------------------------+--------------------------------------+
ubuntu@ubuntu:~$
```

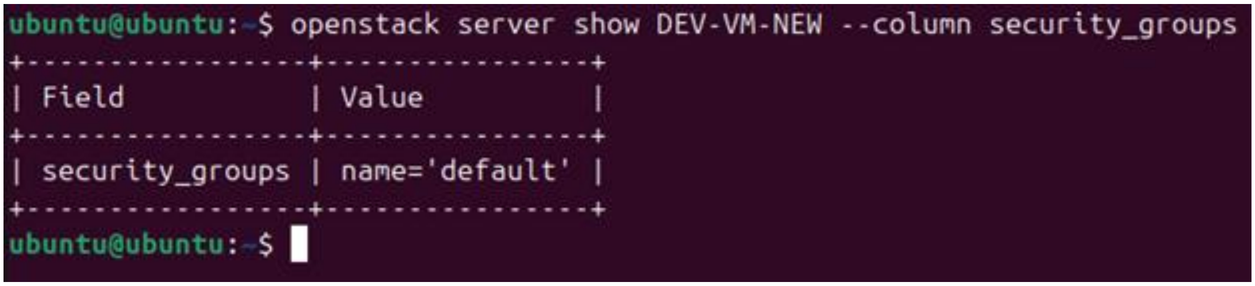
Step 19: Review the security group by typing “openstack security group show dev-secure":



```
ubuntu@ubuntu:~$ openstack security group show dev-secure
+-----------------+-----------------------------------------------------------------------------------------------------------------------------------------+
| Field           | Value                                                                                                                                   |
+-----------------+-----------------------------------------------------------------------------------------------------------------------------------------+
| created_at      | 2025-12-02T02:02:53Z                                                                                                                    |
| description     | Restricted inbound traffic for Dev project                                                                                              |
| id              | de3421ec-b74e-480b-8b20-e6e9d6b4814f                                                                                                    |
| is_shared       | False                                                                                                                                   |
| name            | dev-secure                                                                                                                              |
| project_id      | 9bf82b31e25e48b7964186df6f3f7df0                                                                                                        |
| revision_number | 4                                                                                                                                       |
| rules           | created_at='2025-12-02T02:02:53Z', direction='egress', ethertype='IPv6', id='2ea5694c-2197-46a9-9520-57f8a5c426f0', standard_attr_id='80', |
|                 | updated_at='2025-12-02T02:02:53Z'                                                                                                       |
|                 | created_at='2025-12-02T02:02:53Z', direction='egress', ethertype='IPv4', id='3571fafd-880e-47cd-b918-cd56535b4a26', standard_attr_id='79', |
|                 | updated_at='2025-12-02T02:02:53Z'                                                                                                       |
|                 | created_at='2025-12-02T02:04:05Z', direction='ingress', ethertype='IPv4', id='778a557c-a0b9-4037-a28e-2c976f437224', normalized_cidr='0.0.0.0/0', |
|                 | port_range_max='22', port_range_min='22', protocol='tcp', remote_ip_prefix='0.0.0.0/0', standard_attr_id='81', updated_at='2025-12-02T02:04:05Z' |
|                 | created_at='2025-12-02T02:05:32Z', direction='ingress', ethertype='IPv4', id='d1ebe3d3-5115-4c1c-ad8c-46186bfbbf3e', normalized_cidr='0.0.0.0/0', protocol='icmp', |
|                 | remote_ip_prefix='0.0.0.0/0', standard_attr_id='82', updated_at='2025-12-02T02:05:32Z'                                                  |
|                 | created_at='2025-12-02T02:07:44Z', direction='ingress', ethertype='IPv4', id='ee354ffe-d108-467a-9f9a-9e99912c2273', normalized_cidr='0.0.0.0/0', |
|                 | port_range_max='80', port_range_min='80', protocol='tcp', remote_ip_prefix='0.0.0.0/0', standard_attr_id='83', updated_at='2025-12-02T02:07:44Z' |
| stateful        | True                                                                                                                                    |
| tags            | []                                                                                                                                      |
| updated_at      | 2025-12-02T02:07:44Z                                                                                                                    |
+-----------------+-----------------------------------------------------------------------------------------------------------------------------------------+
ubuntu@ubuntu:~$
```

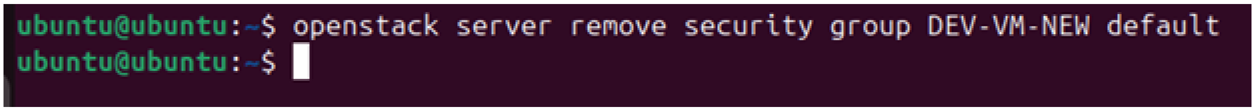
2.5 Applying the Restricted Group to the Dev VM

Step 20: Check the existing groups:



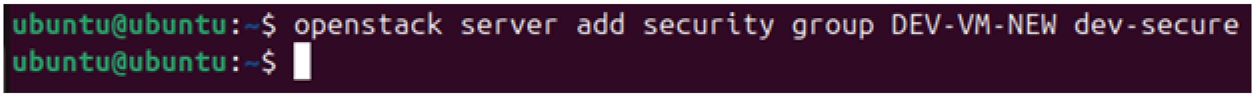
```
ubuntu@ubuntu:~$ openstack server show DEV-VM-NEW --column security_groups
+-----------------+----------------+
| Field           | Value          |
+-----------------+----------------+
| security_groups | name='default' |
+-----------------+----------------+
ubuntu@ubuntu:~$ 
```

Step 21: Remove the default group:



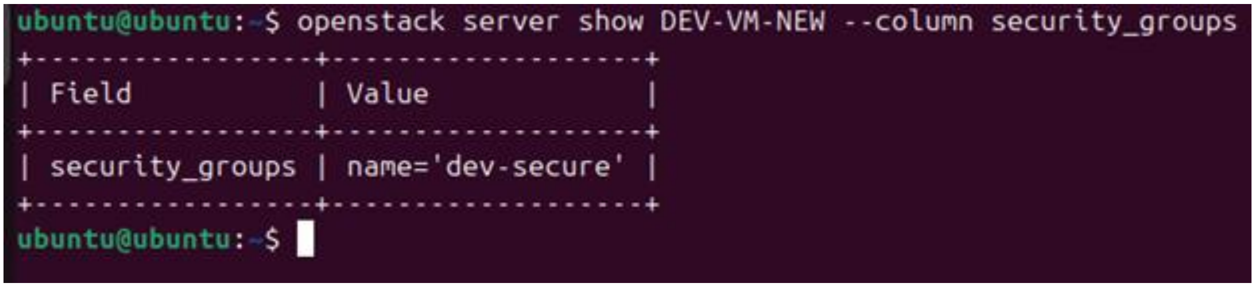
```
ubuntu@ubuntu:~$ openstack server remove security group DEV-VM-NEW default
ubuntu@ubuntu:~$ 
```

Step 22: Add the new group:



```
ubuntu@ubuntu:~$ openstack server add security group DEV-VM-NEW dev-secure
ubuntu@ubuntu:~$ 
```

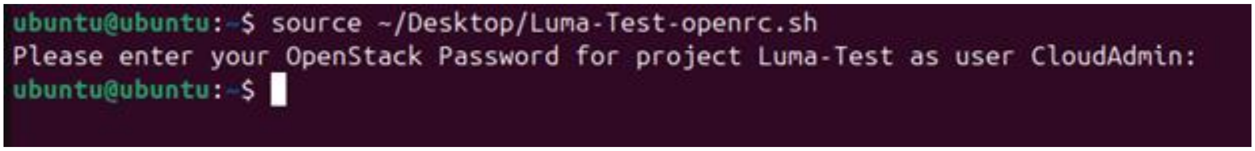
Step 23: Verify the assignment:



```
ubuntu@ubuntu:~$ openstack server show DEV-VM-NEW --column security_groups
+-----------------+-------------------+
| Field           | Value             |
+-----------------+-------------------+
| security_groups | name='dev-secure' |
+-----------------+-------------------+
ubuntu@ubuntu:~$ 
```

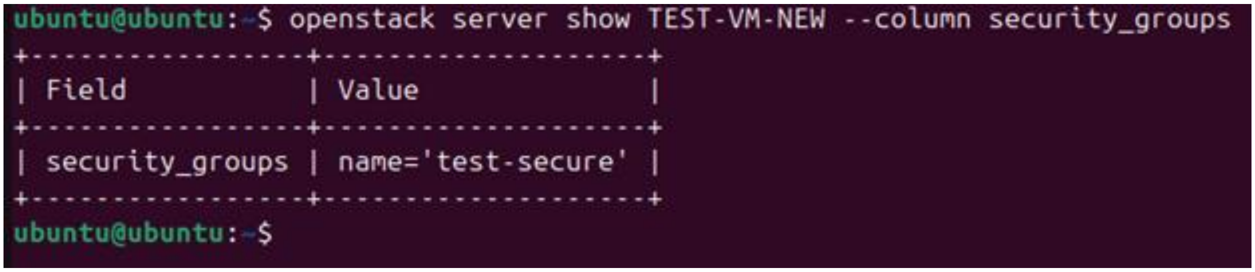
2.6 Validating Security Group Enforcement Across Networks

Step 24: Verify security group rules directly from DevStack CLI:



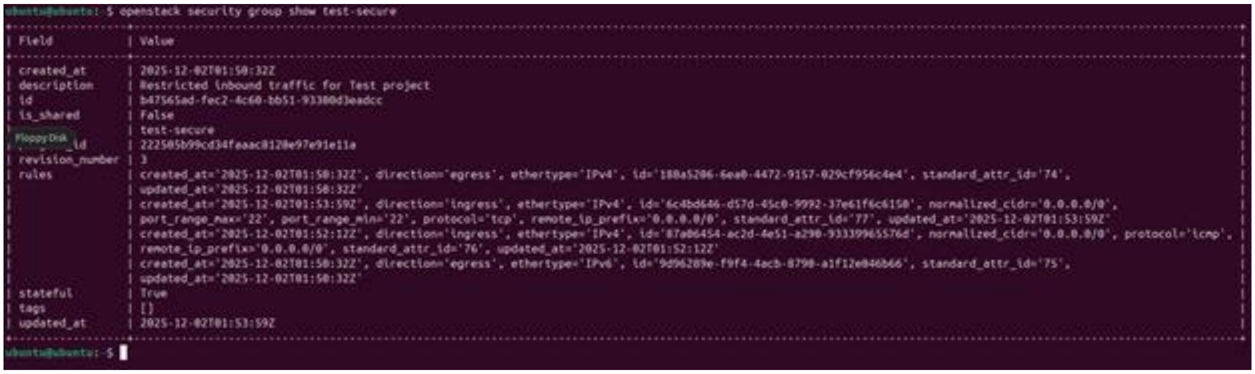
```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Test-openrc.sh
Please enter your OpenStack Password for project Luma-Test as user CloudAdmin:
ubuntu@ubuntu:~$ 
```

Step 25: Show the security group rules in effect for TEST-VM-NEW:



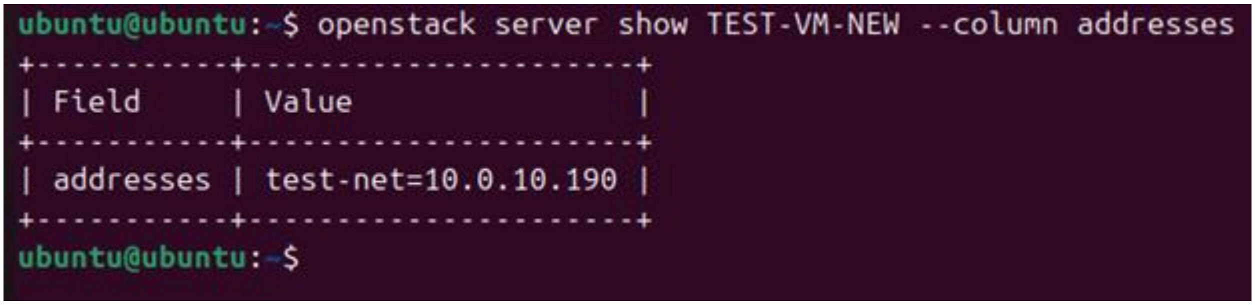
```
ubuntu@ubuntu:~$ openstack server show TEST-VM-NEW --column security_groups
+-----------------+--------------------+
| Field           | Value              |
+-----------------+--------------------+
| security_groups | name='test-secure' |
+-----------------+--------------------+
ubuntu@ubuntu:~$
```

Step 26: View the security group rules by typing “openstack security group show test-secure" into the terminal:

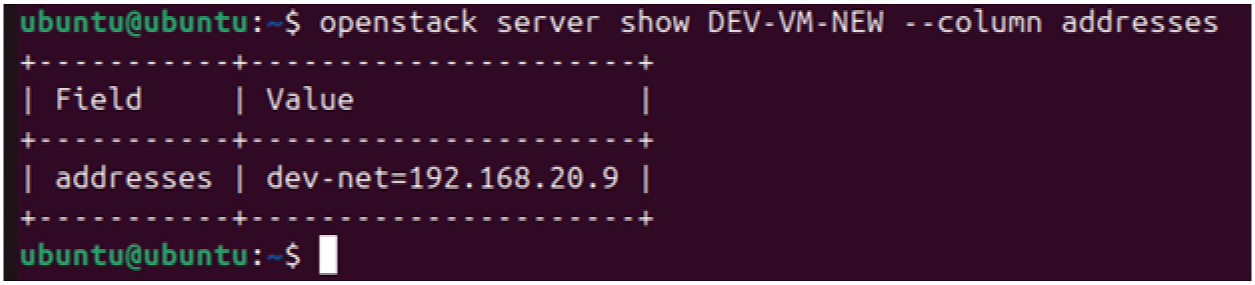


```
ubuntu@ubuntu:~$ openstack security group show test-secure
+-----------------+-----------------------------------------------------------------------------------------------------------------------------------------+
| Field           | Value                                                                                                                                   |
+-----------------+-----------------------------------------------------------------------------------------------------------------------------------------+
| created_at      | 2025-12-02T01:50:32Z                                                                                                                    |
| description     | Restricted inbound traffic for Test project                                                                                             |
| id              | b47565ad-fec2-4c60-bb51-93300d3eadcc                                                                                                    |
| is_shared       | False                                                                                                                                   |
|                 | test-secure                                                                                                                             |
| Floppy Disk _id | 222505b99cd34faaac8120e97e91e11a                                                                                                        |
| revision_number | 3                                                                                                                                       |
| rules           | created_at='2025-12-02T01:50:32Z', direction='egress', ethertype='IPv4', id='188a5206-6ea0-4472-9157-029cf956c4e4', standard_attr_id='74', |
|                 | updated_at='2025-12-02T01:50:32Z'                                                                                                       |
|                 | created_at='2025-12-02T01:53:59Z', direction='ingress', ethertype='IPv4', id='6c4bd646-d57d-45c0-9992-37e61f6c6150', normalized_cidr='0.0.0.0/0', |
|                 | port_range_max='22', port_range_min='22', protocol='tcp', remote_ip_prefix='0.0.0.0/0', standard_attr_id='77', updated_at='2025-12-02T01:53:59Z' |
|                 | created_at='2025-12-02T01:52:12Z', direction='ingress', ethertype='IPv4', id='87a06454-ac2d-4e51-a290-933399655 76d', normalized_cidr='0.0.0.0/0', protocol='icmp', |
|                 | remote_ip_prefix='0.0.0.0/0', standard_attr_id='76', updated_at='2025-12-02T01:52:12Z'                                                  |
|                 | created_at='2025-12-02T01:50:32Z', direction='egress', ethertype='IPv6', id='9d96289e-f9f4-4acb-8790-a1f12e046b66', standard_attr_id='75', |
|                 | updated_at='2025-12-02T01:50:32Z'                                                                                                       |
| stateful        | True                                                                                                                                    |
| tags            | []                                                                                                                                      |
| updated_at      | 2025-12-02T01:53:59Z                                                                                                                    |
+-----------------+-----------------------------------------------------------------------------------------------------------------------------------------+
ubuntu@ubuntu:~$
```

Step 27: Show the network connectivity between VMs:



```
ubuntu@ubuntu:~$ openstack server show TEST-VM-NEW --column addresses
+-----------+----------------------+
| Field     | Value                |
+-----------+----------------------+
| addresses | test-net=10.0.10.190 |
+-----------+----------------------+
ubuntu@ubuntu:~$
```



```
ubuntu@ubuntu:~$ openstack server show DEV-VM-NEW --column addresses
+-----------+----------------------+
| Field     | Value                |
+-----------+----------------------+
| addresses | dev-net=192.168.20.9 |
+-----------+----------------------+
ubuntu@ubuntu:~$
```

2.7 Section Summary

Document the outcomes:

- Replaced permissive defaults: Both projects now use tailored security groups
- Implemented least privilege: Only necessary ports (SSH, ICMP) are open
- Project-specific rules: Dev project has HTTP access, Test project doesn't
- Layered security: Security groups reinforce the network segmentation from Section 1
- Prepared for Section 3: Identity and compute validation

The security posture is now significantly improved with both network isolation AND restrictive firewall rules.

Section 3: Strengthening Compute and Identity Surfaces

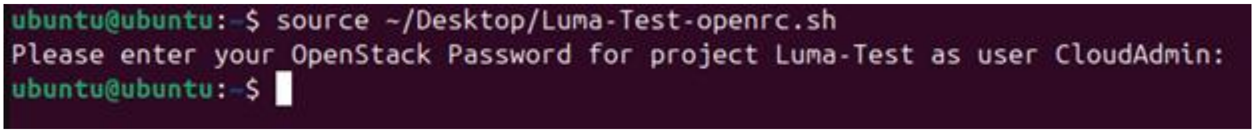
After implementing both segmentation and security rules, our team shifts focus to validating and reinforcing the compute and identity surfaces that support LumaTech's workflows. This phase includes verifying that user roles interact only with the resources assigned to their project and confirming that each instance behaves according to its designated trust boundaries. By testing these interactions from a consultant's perspective, we provide LumaTech with assurance that the deployed controls function cohesively and support the organization's broader security objectives. [6]

3.1 Confirming Project-Level Visibility With User Credentials

Step 1: Start with the Test project:

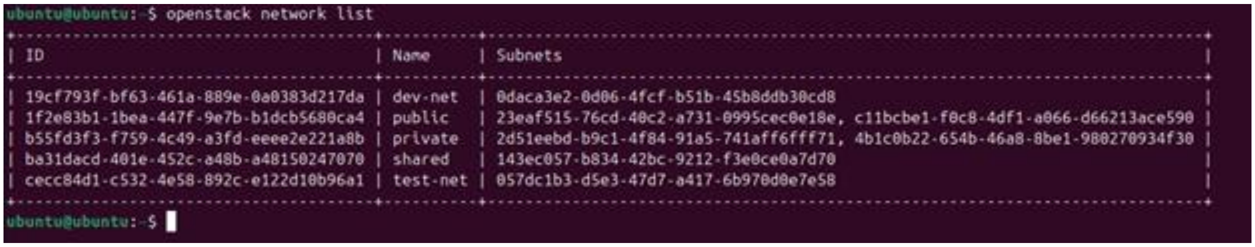
Username: CloudAdmin

Password: password



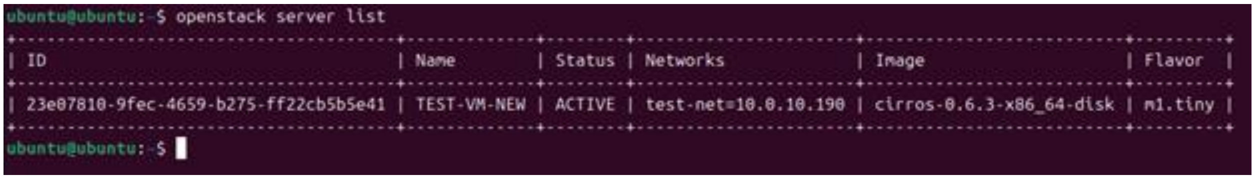
```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Test-openrc.sh
Please enter your OpenStack Password for project Luma-Test as user CloudAdmin:
ubuntu@ubuntu:~$
```

Step 2: List visible networks:



```
ubuntu@ubuntu:~$ openstack network list
+--------------------------------------+----------+----------------------------------------------------------------------------+
| ID                                   | Name     | Subnets                                                                    |
+--------------------------------------+----------+----------------------------------------------------------------------------+
| 19cf793f-bf63-461a-889e-0a0383d217da | dev-net  | 0daca3e2-0d06-4fcf-b51b-45b8ddb30cd8                                       |
| 1f2e83b1-1bea-447f-9e7b-b1dcb5680ca4 | public   | 23eaf515-76cd-40c2-a731-0995cec0e18e, c11bcbe1-f0c8-4df1-a066-d66213ace590 |
| b55fd3f3-f759-4c49-a3fd-eeee2e221a8b | private  | 2d51eebd-b9c1-4f84-91a5-741aff6fff71, 4b1c0b22-654b-46a8-8be1-980270934f30 |
| ba31dacd-401e-452c-a48b-a48150247070 | shared   | 143ec057-b834-42bc-9212-f3e0ce0a7d70                                       |
| cecc84d1-c532-4e58-892c-e122d10b96a1 | test-net | 057dc1b3-d5e3-47d7-a417-6b970d0e7e58                                       |
+--------------------------------------+----------+----------------------------------------------------------------------------+
ubuntu@ubuntu:~$ 
```

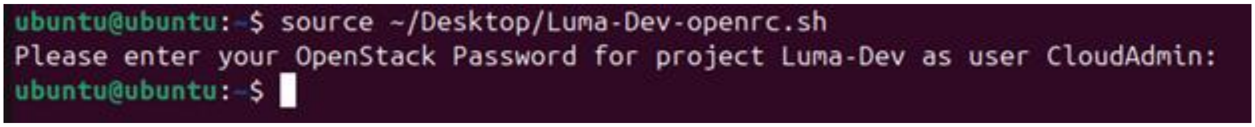
Step 3: List visible instances:



```
ubuntu@ubuntu:~$ openstack server list
+--------------------------------------+-------------+--------+----------------------+--------------------------+---------+
| ID                                   | Name        | Status | Networks             | Image                    | Flavor  |
+--------------------------------------+-------------+--------+----------------------+--------------------------+---------+
| 23e07810-9fec-4659-b275-ff22cb5b5e41 | TEST-VM-NEW | ACTIVE | test-net=10.0.10.190 | cirros-0.6.3-x86_64-disk | m1.tiny |
+--------------------------------------+-------------+--------+----------------------+--------------------------+---------+
ubuntu@ubuntu:~$ 
```

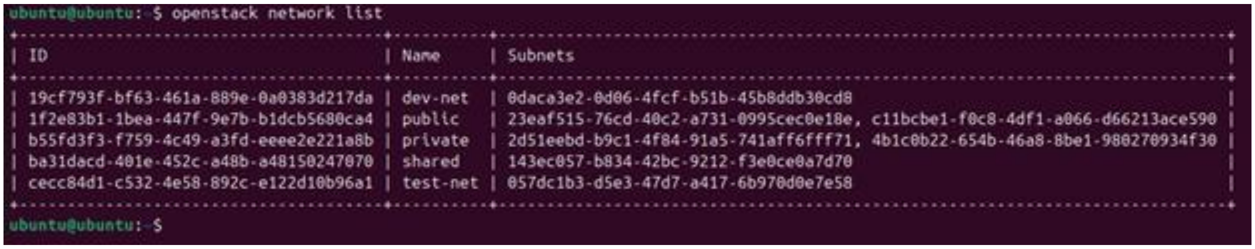
Verify that only Test-owned resources appear. [6]

Step 4: Repeat for the Dev project:



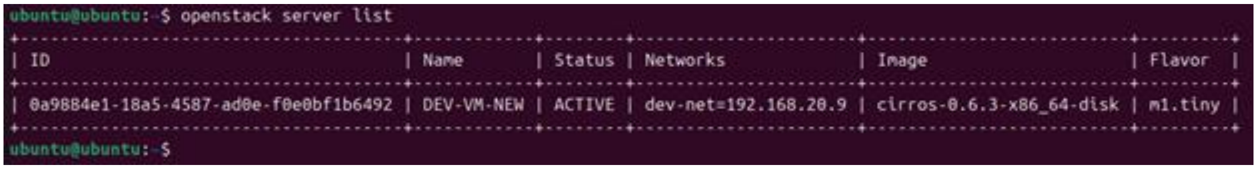
```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Dev-openrc.sh
Please enter your OpenStack Password for project Luma-Dev as user CloudAdmin:
ubuntu@ubuntu:~$ 
```

Step 5: View all networks by typing "openstack network list" into the terminal:



```
ubuntu@ubuntu:~$ openstack network list
+--------------------------------------+----------+----------------------------------------------------------------------------+
| ID                                   | Name     | Subnets                                                                    |
+--------------------------------------+----------+----------------------------------------------------------------------------+
| 19cf793f-bf63-461a-889e-0a0383d217da | dev-net  | 0daca3e2-0d06-4fcf-b51b-45b8ddb30cd8                                       |
| 1f2e83b1-1bea-447f-9e7b-b1dcb5680ca4 | public   | 23eaf515-76cd-40c2-a731-0995cec0e18e, c11bcbe1-f0c8-4df1-a066-d66213ace590 |
| b55fd3f3-f759-4c49-a3fd-eeee2e221a8b | private  | 2d51eebd-b9c1-4f84-91a5-741aff6fff71, 4b1c0b22-654b-46a8-8be1-980270934f30 |
| ba31dacd-401e-452c-a48b-a48150247070 | shared   | 143ec057-b834-42bc-9212-f3e0ce0a7d70                                       |
| cecc84d1-c532-4e58-892c-e122d10b96a1 | test-net | 057dc1b3-d5e3-47d7-a417-6b970d0e7e58                                       |
+--------------------------------------+----------+----------------------------------------------------------------------------+
ubuntu@ubuntu:~$
```

Step 6: View all instances by typing "openstack server list" into the terminal:

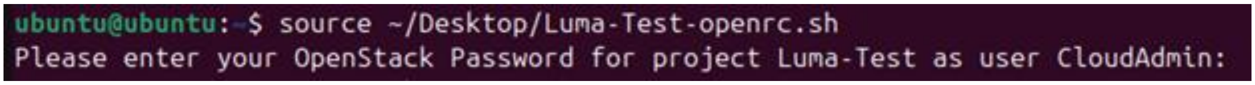


```
ubuntu@ubuntu:~$ openstack server list
+--------------------------------------+-------------+--------+----------------------+--------------------------+---------+
| ID                                   | Name        | Status | Networks             | Image                    | Flavor  |
+--------------------------------------+-------------+--------+----------------------+--------------------------+---------+
| 0a9884e1-18a5-4587-ad0e-f0e0bf1b6492 | DEV-VM-NEW  | ACTIVE | dev-net=192.168.20.9 | cirros-0.6.3-x86_64-disk | m1.tiny |
+--------------------------------------+-------------+--------+----------------------+--------------------------+---------+
ubuntu@ubuntu:~$
```

Notice that each project can only see its own networks and instances, confirming identity-scoped visibility.

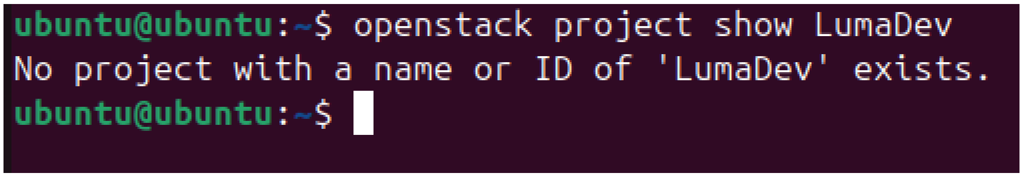
3.2 Verifying Instance Access Behavior Based on Roles

Step 7: Using Test project credentials, attempt to view Dev project details:



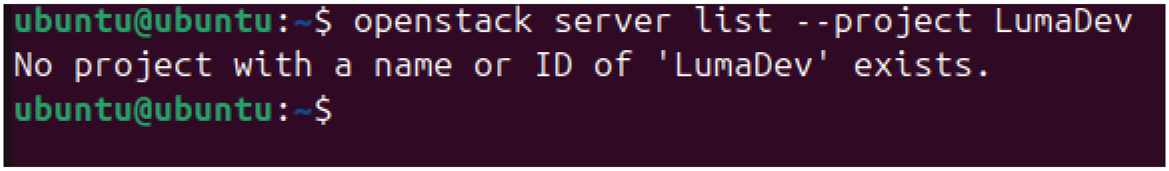
```
ubuntu@ubuntu:~$ source ~/Desktop/Luma-Test-openrc.sh
Please enter your OpenStack Password for project Luma-Test as user CloudAdmin:
```

Step 8: Attempt to view the Dev project:



```
ubuntu@ubuntu:~$ openstack project show LumaDev
No project with a name or ID of 'LumaDev' exists.
ubuntu@ubuntu:~$
```

Step 9: Attempt to list Dev project servers:



```
ubuntu@ubuntu:~$ openstack server list --project LumaDev
No project with a name or ID of 'LumaDev' exists.
ubuntu@ubuntu:~$
```

Expected outcome:

- Access should be denied for all Dev-scoped resources. [6][5]
- Repeat this process from the Dev project attempting to view Test-scoped resources.
- Document any unexpected access.

3.3 Section Summary and Lab Conclusion

- **Identity isolation confirmed**: Each project user can only access resources within their assigned scope
- **Compute boundaries enforced**: VMs cannot access networks or security groups from other projects
- **Cross-project access blocked**: All attempts to access resources across project boundaries are properly denied
- **Layered security validated**: Network, firewall, and identity controls work together cohesively
- **Zero-trust model achieved**: No implicit trust between projects, all access is explicitly controlled [1]

Mission accomplished: LumaTech's cloud environment has been transformed from a vulnerable shared infrastructure to a properly segmented, secure multi-tenant environment that prevents lateral movement and enforces strict project isolation.

References

[1] NIST, *Zero Trust Architecture (SP 800-207)*, Aug. 2020.
Available: https://doi.org/10.6028/NIST.SP.800-207

[2] NIST, *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*, Sept. 2020.
Available: https://doi.org/10.6028/NIST.SP.800-53r5

[3] OpenStack Foundation, *OpenStack Networking (Neutron) Admin Guide*, 2024.
Available: https://docs.openstack.org/neutron/latest/admin/

[4] OpenStack Foundation, *OpenStack Compute (Nova) Administration Guide*, 2024.
Available: https://docs.openstack.org/nova/latest/

[5] OpenStack Foundation, *OpenStack Security Guide*, 2024.
Available: https://docs.openstack.org/security-guide/

[6] OpenStack Foundation, *Identity Service (Keystone) Documentation*, 2024.
Available: https://docs.openstack.org/keystone/latest/

[7] OpenStack Foundation, *Security Groups — Neutron*, 2024.
Available: https://docs.openstack.org/neutron/latest/admin/security-groups.html