Linux Academy

Live! Lab

Configure Access and Security for Instances

Contents

Lab Connection Information

- Labs may take up to five minutes to build
- Access to the Horizon Dashboard is provided on the Live! Lab page, along with your login credentials
- SSH information is provided on the Live! Lab page
- Labs will automatically end once the alloted amount of time finishes

Related Courses

OpenStack Foundation Certifed Administrator

Related Videos

Manage Project Security Group Rules

Assign a Security Group to an Instance

Access an Instance Using a Key Pair

Need Help?

Linux Academy Community

... and you can always send in a support ticket on our website to talk to an instructor!

Introduction

When we create virtual machines, we want to ensure they are secure. This lab covers two ways in which we can secure our servers: Through the use of a key pair, and through OpenStack security groups.

Log in to the Horizon Dashboard as the *demo* tenant, navigating to **Access & Security** Go to the **API Access** tab, then **Download OpenStack RC File**.

Using the provided SSH Details, log in to the server from your terminal. Either copy the OpenStack RC file to a new file named *demo.sh* or `scp` the file to the server, ensuring *demo.sh* is the file's name.

Source the file, inputting your *demo* user's password when prompted:

```
root@openstack:~# source demo.sh
```

Creating a Key Pair

To securely access any virtual machines, we need to create a key pair using `nova`:

```
root@openstack:~# nova keypair-add key > key.pem
```

`ls` to view the created *key.pem* file, then change permissions:

```
root@openstack:~# chmod 600 key.pem
```

To ensure nova has access to the key pair, run:

```
root@openstack:~# nova keypair-list
+------+------+-------------------------------------------------+
| Name | Type | Fingerprint                                     |
+------+------+-------------------------------------------------+
| key  | ssh  | 4f:1b:98:71:7f:89:64:dc:c4:7d:1f:69:0b:e1:72:cf |
+------+------+-------------------------------------------------+
```

Creating a Security Group

With our key pair added with `nova`, we now need to add a security group. To view the current security groups, run:

```
root@openstack:~# nova secgroup-list
+--------------------------------------+---------+------------------------+
| Id                                   | Name    | Description            |
+--------------------------------------+---------+------------------------+
| 0141e32d-d153-4646-a091-c863f1c3b680 | default | Default security group |
+--------------------------------------+---------+------------------------+
```

A *default* security group is already available, but we are creating our own. In this instance, we are creating one for our web servers. Create the initial group:

```
root@openstack:~# nova secgroup-create webserversg "Security group for web servers"
+--------------------------------------+-------------+---------------------------------+
| Id                                   | Name        | Description                     |
+--------------------------------------+-------------+---------------------------------+
| d7ad8471-29cf-4ee7-ac41-e52af83f28e4 | webserversg | Security group for web servers |
+--------------------------------------+-------------+---------------------------------+
```

`webserversg` is the name we gave the security group, whereas the words contained between quotes are the description.

Should you view the list of security groups again, the new *webserversg* group is now available.

Adding Firewall Rules

To view the default firewall rules for our newly-created *webserversg* security group, use the `nova secgroup-list-rules` command:

```
root@openstack:~# nova secgroup-list-rules webserversg
+-------------+-----------+---------+-----------+--------------+
| IP Protocol | From Port | To Port | IP Range  | Source Group |
+-------------+-----------+---------+-----------+--------------+
+-------------+-----------+---------+-----------+--------------+
```

Currently, we do not have any rules. We want to add a rule for SSH access:

```
root@openstack:~# nova secgroup-add-rule webserversg tcp 22 22 0.0.0.0/0
+-------------+-----------+---------+-----------+--------------+
| IP Protocol | From Port | To Port | IP Range  | Source Group |
+-------------+-----------+---------+-----------+--------------+
| tcp         | 22        | 22      | 0.0.0.0/0 |              |
+-------------+-----------+---------+-----------+--------------+
```

The command defines the security group we are working with (`webserversg`), the protocol we are using (`tcp`) the **from** and **to** ports (`22` and `22`), and the CIDR block notation from which to accept connections from. `0.0.0.0/0` allows connections from anywhere, but if you are connecting from a single IP address, this can be fine-tuned for additional security.

If we view the rules for our *webserversg* group now, we can see that port 22 is open.

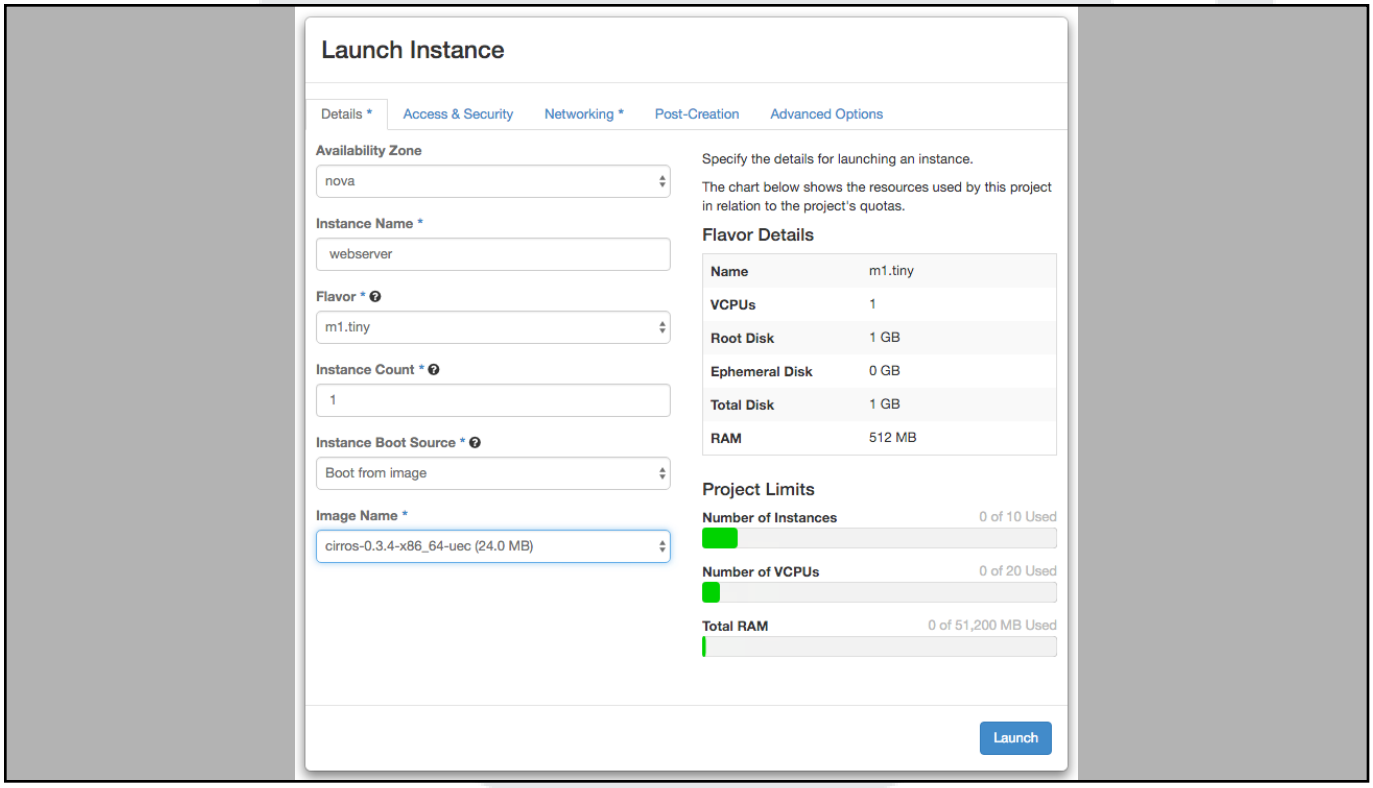
We also want to allow *icmp* to ping servers:

```
root@openstack:~# nova secgroup-add-rule webserversg icmp -1 -1 0.0.0.0/0
+-------------+-----------+---------+-----------+--------------+
| IP Protocol | From Port | To Port | IP Range  | Source Group |
+-------------+-----------+---------+-----------+--------------+
| icmp        | -1        | -1      | 0.0.0.0/0 |              |
+-------------+-----------+---------+-----------+--------------+
```

Launching a Secure Instance

To test SSH access, we need to spin up a new instance using the *webserversg* security group.

Return to the Horizon Dashboard, and select **Instances**, under **Compute**. Click **Launch Instance**.



From the **Details** tab, give the instance a **Name** of *webserver*, a **Flavor** of *m1.tiny*, and an **Instance Count** of *1*. Set the **Instance Boot Source** to *Boot from image*, and select the *cirros-* image from the **Image Name** list. Do not launch.

Go to the **Access & Security** tab, and ensure the *key* key pair is selected. Select the *webserversg* **Security Group**. Move to the **Networking** tab to ensure the *private* network is selected. **Launch**.

With the instance up and running, return to the terminal and run:

```
root@openstack:~# nova list
+--------------+-----------+--------+------------+-------------+-----------------------+
| ID           | Name      | Status | Task State | Power State | Networks              |
+--------------+-----------+--------+------------+-------------+-----------------------+
| 2812fb94-5c05 | webserver | ACTIVE | -          | Running     | private=fda9, 10.0.0.3 |
+--------------+-----------+--------+------------+-------------+-----------------------+
```

You can see that your new instance is active, and located at the private IP of *10.0.0.3*. Test that you can ping the server:

```
root@openstack:~# ping 10.0.0.3
```

Using the Key Pair & Deleting Security Groups

SSH into the Instance

From the terminal, we can now use the *key.pem* key pair to SSH into the new instance:

```
root@openstack:~# ssh -i key.pem cirros@10.0.0.3
```

You are now in the new instance. Exit:

```
$ exit
```

Deleting Security Group

Before we delete the security group, we need to remove the instance using it. Return to the Horizon Dashboard, navigating to the **Instances** page. Select and **Terminate Instace[s]**.

Once terminated, return to the terminal. View your security groups:

```
root@openstack:~# nova secgroup-list
+--------------------------------------+-------------+---------------------------------+
| Id                                   | Name        | Description                     |
+--------------------------------------+-------------+---------------------------------+
| 0141e32d-d153-4646-a091-c863f1c3b680 | default     | Default security group          |
| d7ad8471-29cf-4ee7-ac41-e52af83f28e4 | webserversg | Security group for web servers |
+--------------------------------------+-------------+---------------------------------+
```

To delete the *webserversg* instance, run:

```
root@openstack:~# nova secgroup-delete webserversg
+--------------------------------------+-------------+---------------------------------+
| Id                                   | Name        | Description                     |
```

```
+--------------------------------------+-------------+--------------------------------+
| d7ad8471-29cf-4ee7-ac41-e52af83f28e4 | webserversg | Security group for web servers |
+--------------------------------------+-------------+--------------------------------+
```

List the security groups again; only the *default* group should be available.