# Method of Procedure (MOP) for Installing a VM in OpenStack and Configuring Firewall

## Title: OpenStack VM Installation and Firewall Configuration

### Date: 2024-06-05

### Reference

- OpenStack Documentation: https://docs.openstack.org/

- Firewall Configuration Guide: https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-20-04

### Prerequisites

- Access to an OpenStack environment with appropriate permissions to create and manage instances.

- OpenStack CLI or Horizon dashboard access.

- Basic knowledge of networking and firewall concepts.

### Objective

To create a virtual machine (VM) in OpenStack, assign a specific IP address, and configure a firewall to block all traffic except for specified ports.

### Procedure

#### Step 1: Create a VM in OpenStack

1. \*\*Log in to OpenStack:\*\*

- Use the OpenStack CLI or Horizon dashboard to log in.

2. \*\*Select the appropriate project:\*\*

- Ensure you are in the correct project where you want to create the VM.

3. \*\*Create a VM:\*\*

- Using the OpenStack CLI, run the following command to create a VM:

```bash

openstack server create --flavor <FLAVOR\_NAME> --image <IMAGE\_NAME> --network <NETWORK\_NAME> --key-name <KEY\_NAME> --security-group <SECURITY\_GROUP\_NAME> <VM\_NAME>

```

- Replace `<FLAVOR\_NAME>`, `<IMAGE\_NAME>`, `<NETWORK\_NAME>`, `<KEY\_NAME>`, `<SECURITY\_GROUP\_NAME>`, and `<VM\_NAME>` with your specific values.

4. \*\*Assign a specific IP address:\*\*

- To assign a specific floating IP, first allocate a floating IP:

```bash

openstack floating ip create <EXTERNAL\_NETWORK>

```

- Then associate the floating IP with your VM:

```bash

openstack floating ip set --port <PORT\_ID> <FLOATING\_IP>

```

- Replace `<EXTERNAL\_NETWORK>`, `<PORT\_ID>`, and `<FLOATING\_IP>` with your specific values.

#### Step 2: Configure Firewall

1. \*\*Access the VM:\*\*

- SSH into the VM using the floating IP:

```bash

ssh -i <KEY\_PATH> <USERNAME>@<FLOATING\_IP>

```

2. \*\*Install UFW (Uncomplicated Firewall):\*\*

- Update the package list and install UFW:

```bash

sudo apt update

sudo apt install ufw

```

3. \*\*Set default policies:\*\*

- Block all incoming traffic by default:

```bash

sudo ufw default deny incoming

```

- Allow all outgoing traffic:

```bash

sudo ufw default allow outgoing

```

4. \*\*Allow specific ports:\*\*

- Allow traffic on specific ports (e.g., SSH on port 22, HTTP on port 80, and HTTPS on port 443):

```bash

sudo ufw allow 22/tcp

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

```

5. \*\*Enable UFW:\*\*

- Enable the firewall:

```bash

sudo ufw enable

```

6. \*\*Check UFW status:\*\*

- Verify the firewall rules:

```bash

sudo ufw status

```

#### Step 3: Set CPU and RAM for the VM

1. \*\*Modify the flavor (if necessary):\*\*

- If you need to change the CPU or RAM after the VM is created, you may need to create a new flavor or resize the existing one.

- To create a new flavor:

```bash

openstack flavor create --ram <RAM\_MB> --disk <DISK\_GB> --vcpus <VCPUS> <FLAVOR\_NAME>

```

- Replace `<RAM\_MB>`, `<DISK\_GB>`, `<VCPUS>`, and `<FLAVOR\_NAME>` with your desired specifications.

2. \*\*Resize the VM:\*\*

- To resize the existing VM to a new flavor:

```bash

openstack server resize --flavor <NEW\_FLAVOR\_NAME> <VM\_NAME>

```

- Confirm the resize:

```bash

openstack server resize confirm <VM\_NAME>

```

### Conclusion

This MOP outlines the steps to create a VM in OpenStack, assign a specific IP address, and configure a firewall to restrict traffic. Additionally, it provides guidance on how to set CPU and RAM specifications for the VM. Always ensure to follow best practices for security and resource management in your OpenStack environment.