# Method of Procedure (MOP) for Deploying a VM on OpenStack with Specific Configuration

## Title: Deploying a VM on OpenStack with Specific Resources and Firewall Configuration

### Date: 2024-06-05

### Reference:

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

- OpenStack CLI Reference: https://docs.openstack.org/python-openstackclient/latest/

### Prerequisites:

1. Access to an OpenStack environment with appropriate permissions to create VMs.

2. OpenStack CLI installed and configured on your local machine or access to the OpenStack dashboard.

3. Knowledge of the specific subnet and IP address to be assigned to the VM.

### Objective:

To deploy a VM on OpenStack with specific memory, CPU, and IP address, and configure a firewall to block all traffic except for a designated subnet.

### Procedure:

#### Step 1: Log in to OpenStack

1. Open your terminal or command prompt.

2. Source your OpenStack credentials:

```bash

source /path/to/your/openrc.sh

```

#### Step 2: Define Variables

1. Define the following variables in your terminal:

```bash

NODE\_NAME="your\_node\_name" # Specify the desired node name

FLAVOR="m1.small" # Specify the flavor (e.g., m1.small for 2GB RAM, 1 vCPU)

IMAGE="ubuntu-22.04" # Specify the image name

NETWORK="your\_network\_name" # Specify the network name

IP\_ADDRESS="192.168.122.10" # Specify the desired static IP address

SECURITY\_GROUP="default" # Specify the security group

```

#### Step 3: Create the VM

1. Create the VM using the OpenStack CLI:

```bash

openstack server create --flavor $FLAVOR --image $IMAGE --nic net-id=$NETWORK,port-id=$(openstack port create --network $NETWORK --fixed-ip address=$IP\_ADDRESS --format value -c id) --security-group $SECURITY\_GROUP --key-name your\_key\_name $NODE\_NAME

```

#### Step 4: Configure the Firewall

1. SSH into the newly created VM:

```bash

ssh your\_username@$IP\_ADDRESS

```

2. Install `ufw` (Uncomplicated Firewall) if not already installed:

```bash

sudo apt update

sudo apt install ufw

```

3. Configure the firewall to allow traffic only from a specific subnet (e.g., `192.168.122.0/24`):

```bash

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow from 192.168.122.0/24

```

4. Enable the firewall:

```bash

sudo ufw enable

```

5. Check the status of the firewall to ensure the rules are applied:

```bash

sudo ufw status verbose

```

#### Step 5: Verify the Configuration

1. Ensure the VM is running:

```bash

openstack server list

```

2. Verify that the firewall rules are correctly set up by checking the status again:

```bash

sudo ufw status verbose

```

3. Test connectivity from another VM or host within the allowed subnet to ensure that traffic is flowing correctly.

### Conclusion:

You have successfully deployed a VM on OpenStack with specific memory, CPU, and IP address, and configured a firewall to block all traffic except for a designated subnet. Ensure to document the VM details and firewall rules for future reference.

### Notes:

- Adjust the flavor and image according to your requirements.

- Ensure that the specified IP address is available and does not conflict with other devices in the network.

- Modify the security group rules as necessary to allow specific traffic (e.g., SSH, HTTP) if needed.