# Method of Procedure (MOP) for Deploying an OpenStack VM with HAProxy

## Date: 2024-06-05

## Author: [Your Name]

## Reference: OpenStack Documentation

### Prerequisites

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

- OpenStack CLI installed and configured on your local machine or management node.

- A specific node (compute node) where the VM will be deployed.

- Knowledge of the desired static IP address, CPU, and RAM specifications.

### Objective

To deploy an OpenStack VM on a specific node, assign it a static IP, install HAProxy, and configure it to allow only specific ports.

### Steps

#### 1. Prepare the Environment

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

```bash

source /path/to/your/openrc.sh

```

2. \*\*Identify the Compute Node\*\*:

Use the following command to list available compute nodes:

```bash

openstack hypervisor list

```

#### 2. Create a Flavor

Create a flavor that specifies the desired CPU and RAM for the VM.

```bash

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

```

Example:

```bash

openstack flavor create --ram 2048 --disk 20 --vcpus 2 m1.small

```

#### 3. Create a Network and Subnet

If you do not have an existing network, create one:

```bash

openstack network create <NETWORK\_NAME>

openstack subnet create --network <NETWORK\_NAME> --subnet-range <SUBNET\_CIDR> <SUBNET\_NAME>

```

Example:

```bash

openstack network create my-network

openstack subnet create --network my-network --subnet-range 192.168.1.0/24 my-subnet

```

#### 4. Create a Security Group

Create a security group to allow specific ports (e.g., HTTP, HTTPS).

```bash

openstack security group create <SECURITY\_GROUP\_NAME>

openstack security group rule create --protocol tcp --dst-port 80:80 <SECURITY\_GROUP\_NAME>

openstack security group rule create --protocol tcp --dst-port 443:443 <SECURITY\_GROUP\_NAME>

```

Example:

```bash

openstack security group create my-sec-group

openstack security group rule create --protocol tcp --dst-port 80:80 my-sec-group

openstack security group rule create --protocol tcp --dst-port 443:443 my-sec-group

```

#### 5. Launch the VM

Deploy the VM on the specified compute node with a static IP.

```bash

openstack server create --flavor <FLAVOR\_NAME> --image <IMAGE\_NAME> --network <NETWORK\_NAME> --security-group <SECURITY\_GROUP\_NAME> --key-name <KEY\_NAME> --nic net-id=<NETWORK\_ID>,v4-fixed-ip=<STATIC\_IP> <VM\_NAME>

```

Example:

```bash

openstack server create --flavor m1.small --image Ubuntu-20.04 --network my-network --security-group my-sec-group --key-name my-key --nic net-id=$(openstack network show my-network -f value -c id),v4-fixed-ip=192.168.1.10 my-vm

```

#### 6. Install HAProxy

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

```bash

ssh -i /path/to/your/private\_key.pem ubuntu@192.168.1.10

```

2. \*\*Update the Package List\*\*:

```bash

sudo apt update

```

3. \*\*Install HAProxy\*\*:

```bash

sudo apt install haproxy -y

```

#### 7. Configure HAProxy

1. \*\*Edit the HAProxy Configuration\*\*:

```bash

sudo vi /etc/haproxy/haproxy.cfg

```

2. \*\*Add the Following Configuration\*\*:

```plaintext

frontend http\_front

bind \*:80

acl is\_http path\_beg /

use\_backend http\_back if is\_http

backend http\_back

server web1 192.168.1.20:80 check

server web2 192.168.1.21:80 check

```

3. \*\*Restrict Access to Specific Ports\*\*:

Ensure that only the specified ports are allowed through the firewall:

```bash

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

sudo ufw enable

```

#### 8. Restart HAProxy

```bash

sudo systemctl restart haproxy

```

#### 9. Verify HAProxy Status

Check the status of HAProxy to ensure it is running correctly.

```bash

sudo systemctl status haproxy

```

### Conclusion

You have successfully deployed an OpenStack VM, assigned it a static IP, installed HAProxy, and configured it to allow only specific ports. Ensure to monitor the VM and HAProxy for any issues and adjust configurations as necessary.