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

## Document Control

\*\*Version:\*\* 1.0

\*\*Date:\*\* 2024-06-05

\*\*Author:\*\* [Your Name]

\*\*Reviewed by:\*\* [Reviewer Name]

\*\*Approval:\*\* [Approver Name]

---

## Purpose

This MOP outlines the detailed steps to deploy a Virtual Machine (VM) on OpenStack with specific memory, CPU configuration, and network settings. The VM will have a designated node name, a specific IP address, and a firewall configured to block all traffic except for specified ports.

## Scope

This procedure is applicable to OpenStack environments and assumes that the user has the necessary permissions to create and manage VMs.

## Prerequisites

1. Access to an OpenStack environment with appropriate credentials.

2. OpenStack CLI or Horizon dashboard access.

3. Knowledge of the specific node name, desired IP address, and ports to be allowed through the firewall.

## References

- OpenStack Documentation: [OpenStack User Guide](https://docs.openstack.org/user-guide/)

- OpenStack CLI Reference: [OpenStack CLI Documentation](https://docs.openstack.org/python-openstackclient/latest/)

---

## Procedure

### Step 1: Log in to OpenStack

1. Open a terminal or command prompt.

2. Source your OpenStack credentials:

```bash

source /path/to/your/openrc.sh

```

### Step 2: Create a VM Instance

1. \*\*Define Variables:\*\*

- Set the desired node name, flavor, image, and network.

```bash

NODE\_NAME="your-node-name"

FLAVOR="m1.small" # Adjust based on your requirements

IMAGE="ubuntu-22.04" # Specify the image you want to use

NETWORK="your-network" # Specify the network to attach the VM

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

```

2. \*\*Create the VM:\*\*

Use the OpenStack CLI to create the VM with the specified parameters.

```bash

openstack server create --flavor $FLAVOR --image $IMAGE --nic net-id=$NETWORK --key-name your-key --security-group default --property "name=$NODE\_NAME" --wait --network $NETWORK --block-device-mapping vda="volume-id" --user-data user-data.yaml $NODE\_NAME

```

3. \*\*Assign a Floating IP (if necessary):\*\*

If you need external access, allocate and associate a floating IP.

```bash

FLOATING\_IP=$(openstack floating ip create public -f value -c floating\_ip\_address)

openstack server add floating ip $NODE\_NAME $FLOATING\_IP

```

### Step 3: Configure the VM

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

SSH into the VM using the floating IP or the assigned IP address.

```bash

ssh ubuntu@$IP\_ADDRESS

```

2. \*\*Update the System:\*\*

Update the package list and upgrade installed packages.

```bash

sudo apt update && sudo apt upgrade -y

```

### Step 4: Configure the Firewall

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

If UFW is not installed, install it.

```bash

sudo apt install ufw -y

```

2. \*\*Set Default Policies:\*\*

Block all incoming traffic by default.

```bash

sudo ufw default deny incoming

sudo ufw default allow outgoing

```

3. \*\*Allow Specific Ports:\*\*

Allow traffic on specific ports (e.g., SSH, HTTP, HTTPS).

```bash

sudo ufw allow 22/tcp # SSH

sudo ufw allow 80/tcp # HTTP

sudo ufw allow 443/tcp # HTTPS

```

4. \*\*Enable UFW:\*\*

Enable the firewall.

```bash

sudo ufw enable

```

5. \*\*Check UFW Status:\*\*

Verify the firewall rules.

```bash

sudo ufw status

```

### Step 5: Verify Configuration

1. \*\*Check VM Status:\*\*

Ensure the VM is running.

```bash

openstack server list

```

2. \*\*Test Connectivity:\*\*

From another machine, test connectivity to the VM on allowed ports.

```bash

nc -zv $IP\_ADDRESS 22 # Test SSH

nc -zv $IP\_ADDRESS 80 # Test HTTP

nc -zv $IP\_ADDRESS 443 # Test HTTPS

```

### Step 6: Document the Configuration

1. \*\*Record the VM Details:\*\*

Document the VM name, IP address, and firewall rules for future reference.

---

## Conclusion

This MOP provides a comprehensive guide to deploying a VM on OpenStack with specific configurations, including memory, CPU, IP address, and firewall settings. Ensure to follow each step carefully and verify the configurations to maintain a secure and functional environment.

## Appendices

- \*\*Appendix A:\*\* Troubleshooting Common Issues

- \*\*Appendix B:\*\* Additional Resources and Links

---

\*\*End of Document\*\*