# Method of Procedure (MOP) for Installing a VM in OpenStack, Assigning IP, and Installing Suricata

## Document Control

\*\*Version:\*\* 1.0

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

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

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

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

---

## Purpose

This MOP outlines the steps to create a virtual machine (VM) in OpenStack, assign an IP address, and install Suricata with basic rules configured.

## Scope

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

## Prerequisites

1. Access to an OpenStack environment with appropriate permissions.

2. OpenStack CLI or Horizon dashboard access.

3. Basic knowledge of Linux command line.

## Resources Required

- OpenStack credentials (username, password, project name, and domain).

- A flavor in OpenStack that meets the desired CPU and RAM specifications.

- An image of Ubuntu (preferably 22.04) available in the OpenStack image repository.

## Procedure

### Step 1: Create a Virtual Machine in OpenStack

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

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

2. \*\*Select the desired flavor:\*\*

- List available flavors to choose the desired CPU and RAM configuration.

```bash

openstack flavor list

```

- Note the ID of the flavor you want to use.

3. \*\*Create the VM:\*\*

- Use the following command to create a VM. Replace `<flavor\_id>`, `<image\_id>`, `<network\_id>`, and `<vm\_name>` with your specific values.

```bash

openstack server create --flavor <flavor\_id> --image <image\_id> --network <network\_id> --key-name <key\_name> <vm\_name>

```

4. \*\*Assign an IP Address:\*\*

- After the VM is created, assign a floating IP address if needed.

```bash

openstack floating ip create <external\_network>

openstack server add floating ip <vm\_name> <floating\_ip>

```

### Step 2: Access the VM

1. \*\*SSH into the VM:\*\*

- Use the floating IP to SSH into the VM.

```bash

ssh ubuntu@<floating\_ip>

```

### Step 3: Install Suricata

1. \*\*Update the package list:\*\*

```bash

sudo apt update

```

2. \*\*Install Suricata:\*\*

```bash

sudo apt install suricata -y

```

3. \*\*Configure Suricata:\*\*

- Edit the Suricata configuration file to set basic rules.

```bash

sudo vi /etc/suricata/suricata.yaml

```

- Ensure that the `default-rule-path` is set correctly and that the rules are enabled.

4. \*\*Set Basic Rules:\*\*

- Enable the default rules by ensuring the following line is uncommented in the configuration file:

```yaml

rule-files:

- /etc/suricata/rules/suricata.rules

```

5. \*\*Start Suricata:\*\*

```bash

sudo systemctl start suricata

sudo systemctl enable suricata

```

6. \*\*Verify Suricata is Running:\*\*

```bash

sudo systemctl status suricata

```

### Step 4: Set CPU and RAM as Desired

1. \*\*Change Flavor (if needed):\*\*

- If you need to change the CPU or RAM after the VM is created, you can resize the VM using the following command:

```bash

openstack server resize --flavor <new\_flavor\_id> <vm\_name>

```

- Confirm the resize:

```bash

openstack server resize confirm <vm\_name>

```

2. \*\*Check the new specifications:\*\*

```bash

openstack server show <vm\_name>

```

## Verification

- Ensure that Suricata is running and monitoring traffic.

- Check the Suricata logs for any alerts or issues:

```bash

sudo tail -f /var/log/suricata/suricata.log

```

## Troubleshooting

- If Suricata fails to start, check the configuration file for errors:

```bash

sudo suricata -c /etc/suricata/suricata.yaml --test

```

- Review system logs for any related errors:

```bash

sudo journalctl -xe

```

## Conclusion

This MOP provides a comprehensive guide to creating a VM in OpenStack, installing Suricata, and configuring it with basic rules. Ensure to monitor the Suricata logs and adjust configurations as necessary for optimal performance.

---

\*\*End of Document\*\*