# Method of Procedure (MOP) for Deploying a VM on OpenStack 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 detailed steps to deploy a Virtual Machine (VM) on OpenStack with specific resource allocations (memory and CPU), configure a designated node name, assign a specific IP address, and install Suricata with basic rules.

## Scope

This procedure is intended for system administrators and engineers responsible for managing OpenStack environments and network security.

## Prerequisites

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

2. OpenStack CLI or Horizon dashboard access.

3. Basic knowledge of Linux command line.

4. An Ubuntu 22.04 image available in the OpenStack image repository.

## Resources Required

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

- Ubuntu 22.04 image.

- Network configuration details (specific IP address and network).

## Procedure

### Step 1: Deploy a VM on OpenStack

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

- Open a terminal and source your OpenStack credentials:

```bash

source /path/to/your/openrc.sh

```

2. \*\*Create a VM:\*\*

- Use the following command to create a VM with specific resources. Replace `<NODE\_NAME>`, `<FLAVOR>`, `<IMAGE>`, and `<NETWORK>` with your desired values.

```bash

openstack server create --flavor <FLAVOR> --image <IMAGE> --nic net-id=<NETWORK> --key-name <KEY\_NAME> --security-group <SECURITY\_GROUP> <NODE\_NAME>

```

- Example:

```bash

openstack server create --flavor m1.small --image Ubuntu-22.04 --nic net-id=my-network --key-name my-key --security-group default my-node

```

3. \*\*Assign a Specific IP Address:\*\*

- After the VM is created, assign a specific floating IP address (if required) or configure the fixed IP address in the network settings.

```bash

openstack floating ip create public

openstack server add floating ip <NODE\_NAME> <FLOATING\_IP>

```

### Step 2: Access the VM

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

- Use the following command 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 the following lines are set to enable basic rules:

```yaml

default-rule-path: /var/lib/suricata/rules

```

4. \*\*Download and Enable Basic Rules:\*\*

- Download the Emerging Threats ruleset:

```bash

sudo suricata-update

```

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

```bash

sudo systemctl start suricata

sudo systemctl enable suricata

```

### Step 4: Verify Suricata Installation

1. \*\*Check Suricata Status:\*\*

```bash

sudo systemctl status suricata

```

2. \*\*Test Suricata:\*\*

- Generate some traffic to test Suricata's functionality. You can use tools like `curl` or `ping` to generate traffic.

3. \*\*Check Logs:\*\*

- Review the Suricata logs to ensure it is capturing traffic:

```bash

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

```

### Step 5: Basic Rule Configuration

1. \*\*Create a Basic Rule:\*\*

- Create a custom rule file:

```bash

sudo vi /etc/suricata/rules/local.rules

```

- Add a simple rule to alert on HTTP traffic:

```plaintext

alert http any any -> any any (msg:"HTTP traffic detected"; sid:1000001; rev:1;)

```

2. \*\*Reload Suricata Configuration:\*\*

```bash

sudo suricata-update

sudo systemctl restart suricata

```

### Step 6: Cleanup

1. \*\*Remove the VM (if necessary):\*\*

- If you need to delete the VM after testing:

```bash

openstack server delete <NODE\_NAME>

```

## Conclusion

This MOP provides a comprehensive guide to deploying a VM on OpenStack, configuring it with a specific node name and IP address, and installing Suricata with basic rules. Ensure to monitor Suricata logs for any alerts and adjust rules as necessary for your environment.

## References

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

- Suricata Documentation: https://suricata.readthedocs.io/en/latest/

---

\*\*End of Document\*\*