# MOP (Method of Procedure) - OpenStack에서 VM 배포 및 Suricata 설치

## 문서 개요

이 문서는 OpenStack 환경에서 특정 메모리와 CPU를 가진 VM을 배포하고, 지정된 노드 이름으로 IP 주소를 설정한 후, Suricata를 설치하고 기본 규칙을 설정하는 절차를 상세히 설명합니다.

## 날짜

2024-06-05

## 참조

- OpenStack 공식 문서: https://docs.openstack.org/

- Suricata 설치 가이드: https://suricata-ids.org/docs/

## 사전 준비 사항

1. OpenStack 환경에 접근할 수 있는 권한이 있어야 합니다.

2. OpenStack CLI 또는 Horizon 대시보드에 대한 기본적인 이해가 필요합니다.

3. Ubuntu 22.04 이미지를 사용할 수 있어야 합니다.

## 절차

### 1. VM 생성

1. \*\*OpenStack CLI 또는 Horizon 대시보드에 로그인합니다.\*\*

2. \*\*VM 생성 명령어 실행 (CLI 사용 시):\*\*

```bash

openstack server create --flavor <flavor\_name> --image <image\_name> --key-name <key\_name> --nic net-id=<network\_id> --security-group <security\_group> --user-data <user\_data\_file> <node\_name>

```

- `<flavor\_name>`: 메모리와 CPU가 설정된 플레버 이름 (예: m1.small)

- `<image\_name>`: 사용할 이미지 이름 (예: Ubuntu 22.04)

- `<key\_name>`: SSH 키 이름

- `<network\_id>`: VM이 연결될 네트워크 ID

- `<security\_group>`: VM에 적용할 보안 그룹

- `<user\_data\_file>`: 초기화 스크립트가 포함된 파일 경로

- `<node\_name>`: 사용자가 지정할 VM의 노드 이름

3. \*\*Horizon 대시보드 사용 시:\*\*

- "Instances" 메뉴로 이동하여 "Launch Instance" 버튼 클릭

- 필요한 정보를 입력하고 "Launch Instance" 클릭

### 2. IP 주소 설정

1. \*\*VM이 생성된 후, 고정 IP 주소를 할당합니다.\*\*

- CLI 사용 시:

```bash

openstack server set --property "networks=<network\_name>:<fixed\_ip>" <node\_name>

```

- Horizon 대시보드 사용 시:

- "Instances" 메뉴에서 생성한 VM을 선택하고 "Edit Instance" 클릭

- "Network" 섹션에서 고정 IP 주소를 입력

### 3. Suricata 설치

1. \*\*VM에 SSH로 접속합니다.\*\*

```bash

ssh <username>@<fixed\_ip>

```

2. \*\*Suricata 설치를 위한 패키지 업데이트:\*\*

```bash

sudo apt update

sudo apt upgrade -y

```

3. \*\*Suricata 설치:\*\*

```bash

sudo apt install suricata -y

```

### 4. 기본 규칙 설정

1. \*\*Suricata 기본 규칙 다운로드:\*\*

```bash

sudo suricata-update

```

2. \*\*Suricata 설정 파일 수정:\*\*

- 설정 파일을 열어 기본 규칙을 활성화합니다.

```bash

sudo vi /etc/suricata/suricata.yaml

```

- `default-rule-path`와 `rule-files` 섹션을 확인하고 필요한 규칙 파일이 포함되어 있는지 확인합니다.

3. \*\*Suricata 서비스 시작:\*\*

```bash

sudo systemctl start suricata

sudo systemctl enable suricata

```

### 5. Suricata 상태 확인

1. \*\*Suricata 상태 확인:\*\*

```bash

sudo systemctl status suricata

```

2. \*\*로그 파일 확인:\*\*

```bash

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

```

### 6. 결론

이 문서에서는 OpenStack에서 VM을 배포하고, Suricata를 설치하여 기본 규칙을 설정하는 방법을 설명했습니다. 모든 단계가 성공적으로 완료되면, Suricata가 정상적으로 작동하는지 확인하고, 필요한 경우 추가적인 규칙을 설정하여 보안을 강화할 수 있습니다.