# OpenStack에서 VM 배포 및 방화벽 설정 MOP

## 문서 개요

이 문서는 OpenStack 환경에서 특정 메모리와 CPU를 가진 VM을 배포하고, 사용자 지정 노드 이름 및 IP 주소를 설정하며, 방화벽을 설치하고 특정 포트만 허용하도록 구성하는 절차를 상세히 설명합니다.

## 날짜

2024-06-05

## 참조

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

- 방화벽 설정 관련 문서: https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-20-04

## 사전 준비 사항

1. OpenStack 환경에 접근할 수 있는 사용자 계정이 필요합니다.

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

## 절차

### 1. VM 배포 준비

1. OpenStack에 로그인합니다.

- CLI 사용 시:

```bash

source <your-openrc-file>

```

2. VM 배포에 필요한 변수 설정

- 사용자 지정 노드 이름: `NODE\_NAME`

- 메모리: `2048` MB (2G)

- CPU: `2` cores

- IP 주소: `192.168.1.10` (사용자가 지정한 IP 주소)

### 2. VM 생성

1. OpenStack CLI를 사용하여 VM을 생성합니다.

```bash

openstack server create --flavor m1.small --image <IMAGE\_NAME> --key-name <KEY\_NAME> --nic net-id=<NETWORK\_ID> --security-group <SECURITY\_GROUP> --user-data <USER\_DATA\_FILE> $NODE\_NAME

```

- `<IMAGE\_NAME>`: 사용할 이미지 이름

- `<KEY\_NAME>`: SSH 키 이름

- `<NETWORK\_ID>`: 네트워크 ID

- `<SECURITY\_GROUP>`: 보안 그룹 이름

- `<USER\_DATA\_FILE>`: 초기 설정을 위한 사용자 데이터 파일 (필요 시)

### 3. VM에 접속

1. VM이 생성된 후, SSH를 통해 접속합니다.

```bash

ssh -i <YOUR\_PRIVATE\_KEY> <USERNAME>@192.168.1.10

```

### 4. 방화벽 설치 및 설정

1. UFW(Uncomplicated Firewall) 설치

```bash

sudo apt update

sudo apt install ufw

```

2. 방화벽 기본 설정

```bash

sudo ufw default deny incoming

sudo ufw default allow outgoing

```

3. 특정 포트 허용 (예: SSH, HTTP, HTTPS)

```bash

sudo ufw allow 22 # SSH

sudo ufw allow 80 # HTTP

sudo ufw allow 443 # HTTPS

```

4. 방화벽 활성화

```bash

sudo ufw enable

```

5. 방화벽 상태 확인

```bash

sudo ufw status

```

### 5. VM 설정 확인

1. VM의 메모리 및 CPU 확인

```bash

free -h

lscpu

```

2. IP 주소 확인

```bash

ip a

```

### 6. 완료

- 모든 절차가 완료되면, VM이 정상적으로 배포되고 방화벽이 설정된 것을 확인합니다.

## 주의 사항

- 방화벽 설정 시, 필요한 포트를 미리 확인하고 설정해야 합니다.

- OpenStack 환경에 따라 명령어 및 설정이 다를 수 있으므로, 환경에 맞게 조정해야 합니다.

## 결론

이 문서에서는 OpenStack에서 VM을 배포하고 방화벽을 설정하는 방법을 설명했습니다. 이 절차를 통해 사용자는 특정 요구 사항에 맞는 VM을 쉽게 구성할 수 있습니다.