



# [Openvidu] AWS EC2에서 Openvidu 설정하기



작업 디렉토리: /opt

## 사전 준비

1. 만약 cerbot을 통해 인증서를 받아야 하는 상황이라면, 80번과 443 포트를 사용하는 프로그램이 없어야 한다.
2. ufw 명령어로 방화벽 설정을 해준다.

```
ufw allow ssh

# http
ufw allow 80/tcp
# https
ufw allow 443/tcp

#openvidu용
ufw allow 3478/tcp
ufw allow 3478/udp
ufw allow 40000:57000/tcp
ufw allow 40000:57000/udp
ufw allow 57001:65535/tcp
ufw allow 57001:65535/udp

ufw enable
```

3. `/opt` 디렉토리로 이동
4. openvidu 빌드 패키지 다운로드

```
curl https://s3-eu-west-1.amazonaws.com/aws.openvidu.io/install_openvidu_latest.sh | bash
```

## Openvidu 설정

### 1. openvidu를 설치하고 나면, .env 파일을 수정

```
# Domain name. If you do not have one, the public IP of the machine.
# For example: 198.51.100.1, or openvidu.example.com
DOMAIN_OR_PUBLIC_IP=도메인 or IP 주소

# OpenVidu SECRET used for apps to connect to OpenVidu server and users to access to OpenV
idu Dashboard
OPENVIDU_SECRET=openvidu Secret 입력

# 만약, letsencrypt를 선택하면, 앞에 입력한 도메인 또는 IP로 cert 발급 -> 80포트 사용
CERTIFICATE_TYPE=letsencrypt

# If CERTIFICATE_TYPE=letsencrypt, you need to configure a valid email for notifications
LETSencrypt_EMAIL= 이메일 입력

# Proxy configuration
# If you want to change the ports on which openvidu listens, uncomment the following lines

# letsencrypt로 certificate type을 선택했다면, 초기에는 반드시 80포트 사용
HTTP_PORT=4442

# HTTPS_PORT 변경 -> 앞으로 접속할 포트 넘버
HTTPS_PORT=4443
```

### 2. openvidu 디렉토리에서 docker compose 실행

```
docker compose up -d
```

### 3. 접속: <https://도메인주소:4443> (설정해준 HTTPS 포트)

