

## **Deployment Solution**

## [nginx] nginx를 활용해 AWS EC2에 https 적용하기 (무료 SSL 인증서 발급)

웹사이트에 https 적용하는 이유는 다양합니다. 민감한 통신을 처리하지 않는 경우에도 항상 https를 사용하여 모든 웹사이트를 보호해야 합니다. 웹사이트와 사용자의 개인정 보 모두에 대한 중요한 보안 및 데이터 무결성을 제공하는 것과는 별개로, https는 수많

v https://velog.io/@teveloper/nginx-nginx%EB%A5%BC-%ED%99%9C%EC%9A%A9%ED%95%B4-AWS-EC2%EC%97%90-https-%EC%A0%81%EC%9A%

A9%ED%95%98%EA%B8%B0-%EB%AC%B4%EB%A3%8C-SSL-%EC%9D%B 8%EC%A6%9D%EC%84%9C-%EB%B0%9C%EA%B8%89 이 사이트는 보안 연결(HTTPS)이 사용되었 습니다

비밀번호나 신용카드 번호 등의 정보는 비공개 상태로 이 사 트에 전송됩니다. 자세히 알아보기

☑ 인증서: (유효)

⚠ 오픈비두 서버를 on promises 방식으로 설치할 때, 80포트와 443포트를 사용하고, nginx에서도 80과 443을 사용하여 포트가 겹쳐 둘 다 작동하지 않는게 문제였다.

## 해결방법

1. 오픈비두 서버 포트를 http: 8080 / https: 8443 으로 설정

Deployment Solution 1

```
# 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= zmid ole (letsencrypt 방식을 사용할 것이라면 무조건 도매인 ole!!)
# OpenVidu SECRET used for apps to connect to OpenVidu server and users to access
OPENVIDU_SECRET= 서용자기 지정한 비밀번호 (default: MY_SECRET)
# Certificate type:
# - selfsigned: Self signed certificate. Not recommended for production use.
Users will see an ERROR when connected to web page.
# - owncert: Valid certificate purchased in a Internet services company.
Please put the certificates files inside folder ./owncert
# with names certificate.key and certificate.cert
# - letsencrypt: Generate a new certificate using letsencrypt. Please set the
# required contact email for Let's Encrypt in LETSENCRYPT_EMAIL
CERTIFICATE_TYPE=letsencrypt
# If CERTIFICATE_TYPE=letsencrypt, you need to configure a valid email for notificate.
UETSENCRYPT_EMAIL=_
# Proxy configuration
# If you want to change the ports on which openvidu listens, uncomment the follow
# Allows any request to http://DOMAIN_OR_PUBLIC_IP:HTTPS_PORT/ to be automatically
# redirected to https://DOMAIN_OR_PUBLIC_IP:HTTPS_PORT/
# WARNING: the default port 80 cannot be changed during the first boot
# if you have chosen to deploy with the option CERTIFICATE_TYPE=letsencrypt
HTTP_PORT=8080
# Changes the port of all services exposed by OpenVidu.
# SDKs, REST clients and browsers will have to connect to this port
HTTPS_PORT=8443
```

- 🔽 https://도메인 입력했을 경우, 배포한 사이트로 들어갈 수 있게 하기 위한 작업 🖡
- 2. 프로젝트를 https에서 사용하기 위해 무료 SSL 인증서 발급

```
sudo apt-get install letsencrypt
sudo systemctl stop nginx
sudo letsencrypt certonly --standalone -d www제외한 도메인 이름
```

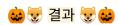
3. /etc/nginx/nginx.conf 파일에 인증서 경로를 포함한 모든 내용 작성

✓ /etc/nginx/sites-enabled/default , ... 등등 여러 파일이 있는데 → 이 모든 파일은
 nginx.conf 파일로 귀속?된다. 다른 파일을 사용할 것이라면 nginx.conf 에 include 로 path를
 지정해줘야 한다.

⇒ 별다른 include를 하지 않고, /etc/nginx/nginx.conf 파일에 모조리 때려넣었다.

Deployment Solution 2

```
worker_processes 1;
events {
   worker_connections 1024;
}
http {
   include
               mime.types;
   default_type application/octet-stream;
    sendfile
                 on;
    keepalive_timeout 65;
    server {
       listen
                   80;
       server_name [YOUR_DOMAIN];
       client_max_body_size 30M;
       keepalive_timeout 5;
       return 301 https://$server_name$request_uri;
    # HTTPS server
    server {
       listen 443 default_server ssl;
       server_name [YOUR DOMMAIN];
       ssl_certificate [YOUR_SSL_CERTIFICATE_LOCATION];
       ssl_certificate_key [YOUR_SSL_CERTIFICATE_KEY_LOCATION];
       ssl_session_cache shared:SSL:1m;
       ssl_session_timeout 5m;
       location / {
            proxy_set_header X-Forwarded-For
                                                $proxy_add_x_forwarded_for;
            proxy_set_header X-Forwarded-Proto https;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header HOST $http_host;
            proxy_set_header X-NginX-Proxy true;
            proxy_pass http://127.0.0.1:[YOUR PORT];
            proxy_redirect off;
       }
   }
}
```





openvidu server : https://도메인:8443

프로젝트 배포 url: https://도메인

Deployment Solution 3