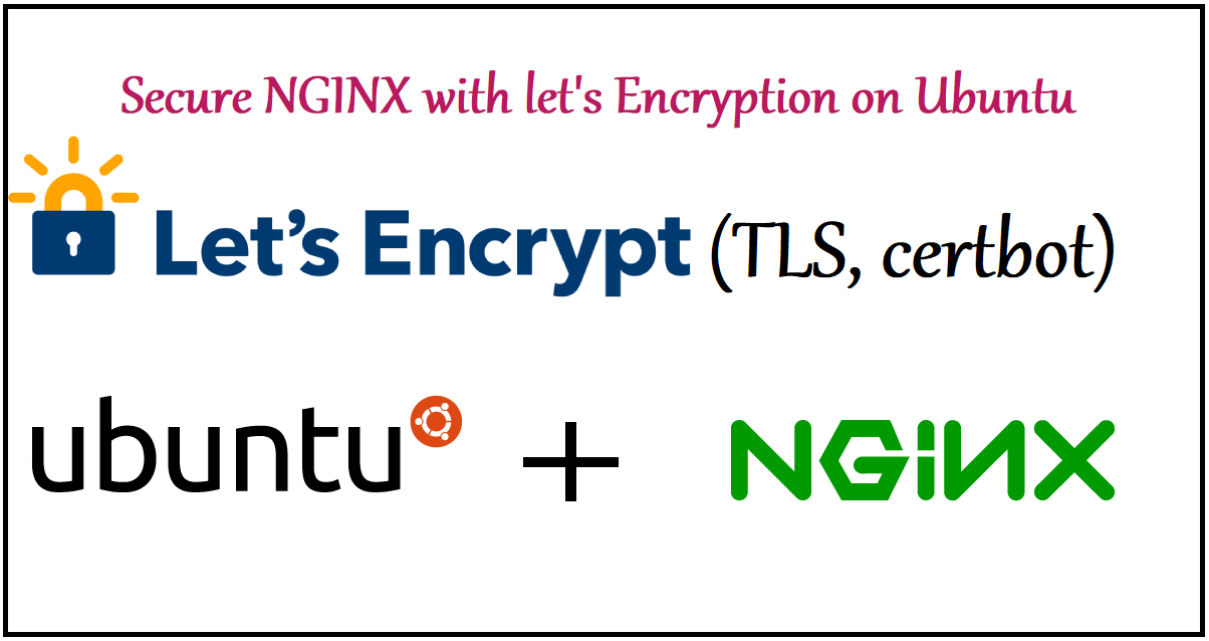
How to add SSL certificate with application Server:

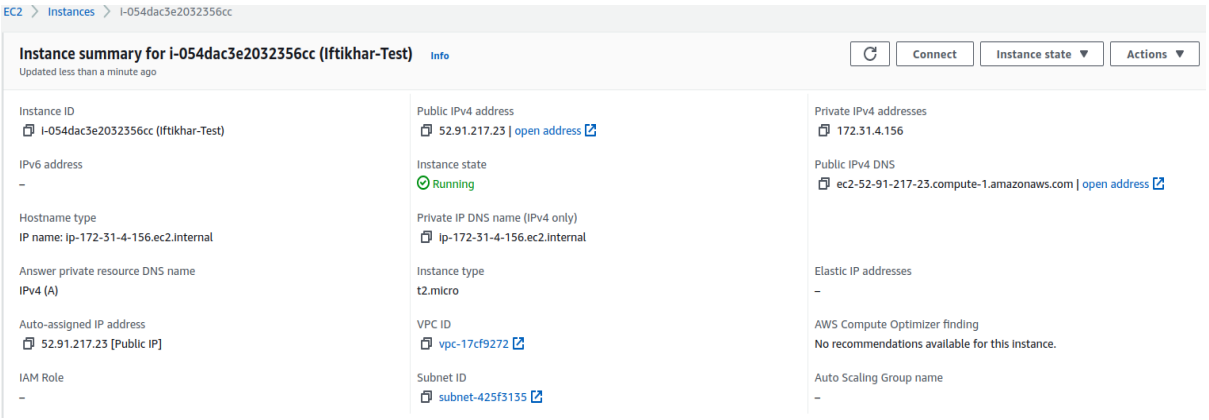
This document will guide how to add an SSL certificate to our application server. We have React Js application that is running over the Amazon EC2 Ubuntu machine. I am assuming you have a basic knowledge of Node JS and Amazon EC2 service.



Following tech we are using in our senrio.

1. Amazon EC2 (Ubuntu Machine)
2. Nginx for Proxy Purpose
3. Node JS
4. React JS App
5. SSL Certificate by using the **Let's Encrypt**

Provisioned EC2 machine using the Ubuntu AMI. Attached the Security group that have HTTP and HTTPS access.



Install the Nginx over the EC2 machine using the following commands:

Update the newly provisioned systems

sudo apt update

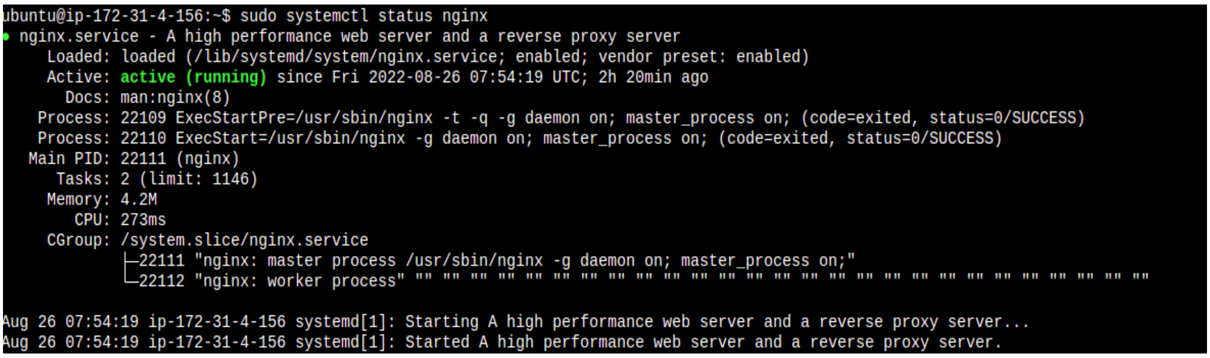
sudo apt upgrade

Install the Nginx service over the machine

sudo apt install nginx

Check the service status

sudo systemctl status nginx



Install Node JS over the EC2 machine:

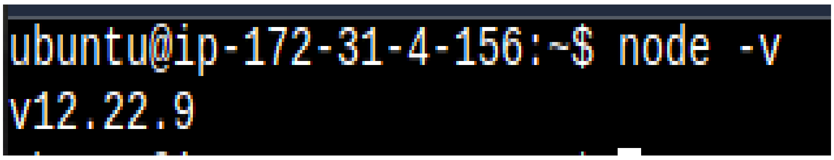
sudo apt install nodejs

Check that the install was successful by querying node for its version number:

node -v

Install `npm`, the Node.js package manager. You can do this by installing the `npm` package with `apt`:

sudo apt install npm



Clone the ReactJS App code over the EC2 Machine using the following command:

git clone https://github.com/sobankhan12/bootcamp-shoe-store.git

Change directory to bootcamp-shoe-store

cd bootcamp-shoe-store/

Then start the npm so it will install the packages that is required for the application and npm will get all the dependencies from packages.json file.

npm start

PM2 is a production process manager for Node.js applications with a built-in load balancer. It allows you to keep applications alive forever, to reload them without downtime and to facilitate common system admin tasks.

npm install pm2 -g

This command will start the ReactJS App at background.

pm2 start npm -- start

The Node JS application will start working on port 3000

PublicIP:3000

Add the Proxy configurations in nginx service default file. So it will redirect the application overthe http and https.

```
location / {
      proxy_pass http://localhost:3000;
      proxy_http_version 1.1;dd
      proxy_set_header Upgrade $http_upgrade;
      proxy_set_header Connection 'upgrade';
      proxy_set_header Host $host;
      proxy_cache_bypass $http_upgrade;
  }
```

The last step is to add the SSL certificate with Nginx service.

https://certbot.eff.org/instructions?ws=nginx&os=ubuntufocal

We will use the Let's Encrypt for generating the SSL certificate.

Install snapd:

Snapd allows upstream software developers to distribute their applications directly to users.

```
sudo apt install snapd
sudo snap install core; sudo snap refresh core
```

Install Certbot

```
sudo snap install --classic certbot
```

Prepare the Certbot command

```
sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

It will add the following configuration over the nginx default file.

```
{
        listen 443 ssl;

        server_name soban.store;

        ssl_certificate /etc/letsencrypt/live/soban.store/fullchain.pem; # managed by Certbot
        ssl_certificate_key /etc/letsencrypt/live/soban.store/privkey.pem; # managed by Certbot

        ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
        ssl_prefer_server_ciphers on;
        ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
```

```
}
```