Arjav Dave Follow
Mar 8, 2021 · 2 min read · Listen

Self-Signed SSL: NGINX on MAC (Part 3)

Nginx From Beginner to Advanced

Till now, we have installed Nginx and did a simple configuration to host an html file locally.

In this part we will be configuring Nginx with a self-signed certificate. We will be creating a self signed certificate using openssl and make Nginx use it for serving content over https. Let's get our hands dirty. Open our pal, Terminal and lets create a couple of folders to store our key and certificate. Fire the following commands:

```
mkdir -p /usr/local/etc/ssl/private
mkdir -p /usr/local/etc/ssl/certs
```

```
sudo openssl req \
  -x509 -nodes -days 365 -newkey rsa:2048 \
  -keyout /usr/local/etc/ssl/private/self-signed.key \
  -out /usr/local/etc/ssl/certs/self-signed.crt
```

Let's alter our server context from previous tutorial. The updated file is as below.

```
events {

}

http {
    server {
        # Listen on port 80 which is the default http port
        listen 80;

        # Set a permanent redirection from http to https
        return 301 https://localhost:443;
    }
}
```

Add another server context inside http context with configuration and locations relating to SSL

```
server {
       listen       443 ssl;

       # location of ssl certificate
       ssl_certificate /usr/local/etc/ssl/certs/self-signed.crt;

       # location of ssl key
       ssl_certificate_key /usr/local/etc/ssl/private/self-
signed.key;
    }
```

Add location context inside the ssl server context

This is the whole configuration file:

```
events {

}

http {
    # HTTP server
    server {
        listen       80;
        return 301 https://localhost:443;
    }

    # HTTPS server
    server {
       listen       443 ssl;

       ssl_certificate /usr/local/etc/ssl/certs/self-signed.crt;
       ssl_certificate_key /usr/local/etc/ssl/private/self-
signed.key;

       location / {
           root   /Users/arjav/Desktop/www;
           index  index.html index.htm;
       }
    }
}
```

As a last step we will need to add the self-signed certificate to the system keychain. Run the below command in your terminal.

```
sudo security add-trusted-cert \
  -d -r trustRoot \
  -k /Library/Keychains/System.keychain
/usr/local/etc/ssl/certs/self-signed.crt
```

Voila! That's it. In your terminal verify your configuration file by running `nginx -t` and if everything looks okay reload your Nginx server by running `nginx -s reload`. Visit https://127.0.0.1. You will still see a red flag or "Not secure" sign in your browser

In the next chapter we will look at some advanced ssl configuration options for better security, caching and optimisation.