Nginx 服务器安装 SSL 证书

环玺信息科技（上海）有限公司

GlobalSign China Co., Ltd

目 录

本文将全面介绍如何在 Nginx 服务器配置 SSL 证书，具体包括在 Nginx 上配置证书文件、证书密钥等参数，以及安装证书后结果的验证。成功配置 SSL 证书后，您将能够通过 HTTPS 加密通道安全访问 Nginx 服务器。

重要：本文以 CentOS 7.9 64 位操作系统、Nginx 1.8.0 为例介绍。不同版本的操作系统或 Web 服务器，部署操作可能有所差异。

前提条件

拥有证书，若您没有证书，请联系您购买证书时所对应的销售人员进行咨询。

- **证书文件：Nginx 支持安装 PEM 格式的文件，PEM 格式的证书文件是采用 Base64 编码的文本文件，且包含完整证书链**
- **私钥文件**

步骤一：在 Nginx 服务器安装证书

1. 执行以下命令，在 Nginx 的 conf 目录下创建一个用于存放证书的目录

```
cd /usr/local/nginx/conf #进入 Nginx 默认配置文件目录。该目录为手动编译安装 Nginx 时的默认目录，如果您修改过默认安装目录或使用其他方式安装，请根据实际配置调整。
mkdir cert #创建证书目录，命名为 cert
```

2. 将证书文件和私钥文件上传到 Nginx 服务器的证书目录（/usr/local/nginx/conf/cert）

3. 编辑 Nginx 配置文件 nginx.conf，修改与证书相关的配置

①. 执行以下命令，打开配置文件

```
vim /usr/local/nginx/conf/nginx.conf
```

重要：nginx.conf 默认保存在/usr/local/nginx/conf 目录下。如果您修改过 nginx.conf 的位置，需将/usr/local/nginx/conf/nginx.conf 进行替换。

②. 在 nginx.conf 中定位到 server 属性配置

```
# HTTPS server
#
#server {
#    listen       443 ssl;
#    server_name  localhost;

#    ssl_certificate      cert.cer;
#    ssl_certificate_key  cert.key;

#    ssl_session_cache    shared:SSL:1m;
#    ssl_session_timeout  5m;

#    ssl_ciphers  HIGH:!aNULL:!MD5;
#    ssl_prefer_server_ciphers  on;

#    location / {
#        root   html;
#        index  index.html index.htm;
#    }
#}
```

③. 删除行首注释符号#，并参考如下示例进行修改

```
server {
    #HTTPS 的默认访问端口 443。
    #如果未在此处配置 HTTPS 的默认访问端口，可能会造成 Nginx 无法启动。
    listen 443 ssl;
    #填写证书绑定的域名
    server_name <yourdomain>;
    #填写证书文件绝对路径
    ssl_certificate cert/<cert-file-name>.cer;
    #填写证书私钥文件绝对路径
    ssl_certificate_key cert/<cert-file-name>.key;
    ssl_session_cache shared:SSL:1m;
    ssl_session_timeout 5m;
    #自定义设置使用的 TLS 协议的类型以及加密套件（以下为配置示例，请您自行评估是否需要配置）
    #TLS 协议版本越高，HTTPS 通信的安全性越高，但是相较于低版本 TLS 协议，高版本 TLS 协议对浏览器的兼容性较差。
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4;
    ssl_protocols TLSv1.1 TLSv1.2 TLSv1.3;
    #表示优先使用服务端加密套件。默认开启
    ssl_prefer_server_ciphers on;
    location / {
        root html;
        index index.html index.htm;
    }
}
```

④. 可选：设置 HTTP 请求自动跳转 HTTPS

如果您希望所有的 HTTP 访问自动跳转到 HTTPS 页面，可通过 rewrite 指令重定向到 HTTPS

重要：以下代码片段需要放置在 nginx.conf 文件中 server {}代码段后面，即设置 HTTP 请求自动跳转 HTTPS 后，nginx.conf 文件中会存在两个 server {}代码段。

```
server {
    listen 80;
    #填写证书绑定的域名
    server_name <yourdomain>;
    #将所有 HTTP 请求通过 rewrite 指令重定向到 HTTPS。
    rewrite ^(.*)$ https://$host$1;
    location / {
        index index.html index.htm;
    }
}
```

配置效果如下图所示

4.执行以下命令，重启 Nginx 服务

```
cd /usr/local/nginx/sbin  #进入 Nginx 服务的可执行目录
./nginx -s reload  #重新载入配置文件
```

说明

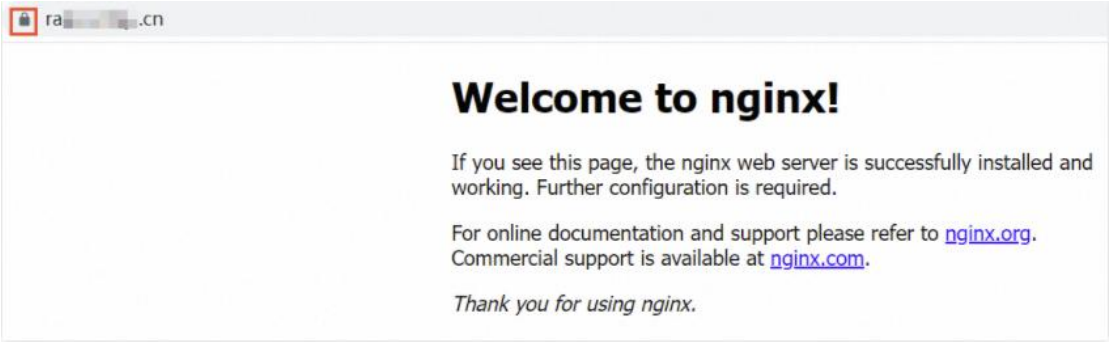
- 报错 `the "ssl" parameter requires ngx_http_ssl_module`：您需要重新编译Nginx并在编译安装的时候加上 `--with-http_ssl_module` 配置。
- 报错 `"/cert/3970497_demo.aliyundoc.com.pem":BIO_new_file() failed (SSL: error:02001002:system library:fopen:No such file or directory:fopen('/cert/3970497_demo.aliyundoc.com.pem','r') error:2006D080:BIO routines:BIO_new_file:no such file)`：您需要去掉证书相对路径最前面的 `/`。例如，您需要去掉 `/cert/cert-file-name.pem` 最前面的 `/`，使用正确的相对路径 `cert/cert-file-name.pem`。

步骤二：验证 SSL 证书是否安装成功

证书安装完成后，您可通过访问证书的绑定域名验证该证书是否安装成功。

```
https://yourdomain    #需要将 yourdomain 替换成证书绑定的域名
```

如果网页地址栏出现小锁标志，表示证书已经安装成功。



技术支持邮箱地址:support-china@globalsign.com

文档支持站点地址:https://www.globalsign.cn/resources/installation