Nginx SSL 证书部署指南

沃通电子认证服务有限公司

WoTrus CA Limited

目　　录

技术支持联系方式

技术支持邮箱：support@wotrus.com

技术支持热线电话：0755-26027828 / 0755-26027859

技术支持网页：https://bbs.wosign.com

公司官网地址：https://www.wosign.com

声明

此文档仅做参考使用，相应的配置需根据当前的配置进行调整。

一、SSL 证书的安装

1.1 获取 SSl 证书

成功在沃通申请证书后，会得到一个有密码的压缩包文件，输入证书密码后解压得到三个文件：**for Apache、for Nginx、for Other Server**，这个是证书的几种格式，**Nginx** 上需要用到 for Nginx 格式的证书。

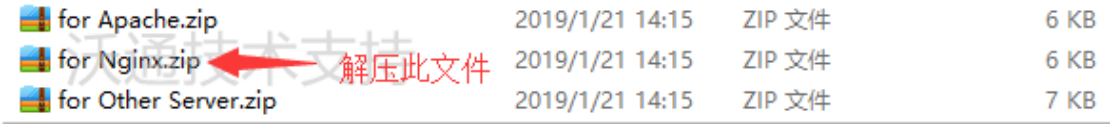

图 1

1. 2 解压证书文件

打开 for Nginx 文件可以看到公钥，如图 2

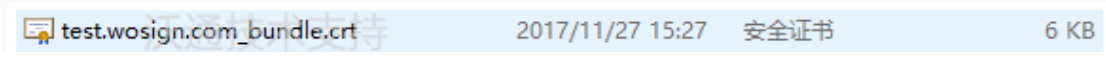

图 2

key 文件，需要找到生成 CSR 一起生成出的两个文件，如图 3

图 3

1.3 安装 SSL 证书

打开 Nginx 安装目录下 conf 目录中的 nginx.conf 文件找到

```
# HTTPS server
    #
```

```
        #server {
        #    listen       443;
        #    server_name  localhost;
        #    ssl                  on;
        #    ssl_certificate    cert.pem;
        #    ssl_certificate_key  cert.key;
        #    ssl_session_timeout  5m;
        #    ssl_protocols  SSLv2 SSLv3 TLSv1;
        #    ssl_ciphers
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
        #    ssl_prefer_server_ciphers   on;
        #    location / {
        #        root   html;
        #        index  index.html index.htm;
        #    }
        #}
```

将其修改为（在 nginx 安装目录下创建 sslkey 目录，将 for Nginx 里面的两个证书文件拷贝到 sslkey 目录下）：

```
        server {
          listen       443;
          server_name  localhost; #（站点域名）
          ssl                  on;
          ssl_certificate      sslkey/wosign.com.crt;      #（证书公钥）
          ssl_certificate_key      sslkey/wosign.com.key; #（证书私钥）
          ssl_session_timeout  5m;
          ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
```

```
ssl_ciphers
    AESGCM:ALL:!DH:!EXPORT:!RC4:+HIGH:!MEDIUM:!LOW:!aNULL:!eNU
  LL;
ssl_prefer_server_ciphers   on;
    location / {
        root   html;
        index  index.html index.htm;
    }
}
```

保存退出，并重启 Nginx。

通过 https 方式访问您的站点，测试站点证书的安装配置。

备注：安装完 ssl 证书后部分服务器可能会有以下错误，请按照链接修复

a. 加密协议和安全套件：https://bbs.wosign.com/thread-1284-1-1.html
b. 部署 https 页面后出现排版错误，或者提示网页有不安全的因素，可参考以下链接：https://bbs.wosign.com/thread-1667-1-1.html

二、SSL 证书的备份

请保存好收到的证书压缩包文件及自己生成 csr 一起的.key 文件，以防丢失

三、SSL 证书的恢复

重复 1.3 操作即可。