
Nginx SSL 证书部署指南



沃通电子认证服务有限公司

WoSignCA Limited

目 录

一、 安装 SSL 证书的环境	3
1.1 SSI 证书安装环境简介	3
1.2 网络环境要求	3
二、 SSL 证书的安装	3
2.1 获取 SSI 证书	3
2.2 解压证书文件	3
2.3 安装 SSL 证书	4
三、 SSL 证书的备份	5
四、 SSL 证书的恢复	5

技术支持联系方式

技术支持邮箱: support@wosign.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、安装 SSL 证书的环境

1.1 SSL 证书安装环境简介

Centos 6.4 操作系统;

Nginx 1.9.1;

Openssl 1.0.1+;

SSL 证书一张 (备注: 本指南使用 s.wosign.com 域名 OV SSL 证书进行操作,通用其它版本证书)。

1.2 网络环境要求

请确保站点是一个合法的外网可以访问的域名地址, 可以正常通过或 `http://XXX` 进行正常访问。

二、SSL 证书的安装

2.1 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五个文件: **for Apache**、**for IIS**、**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。

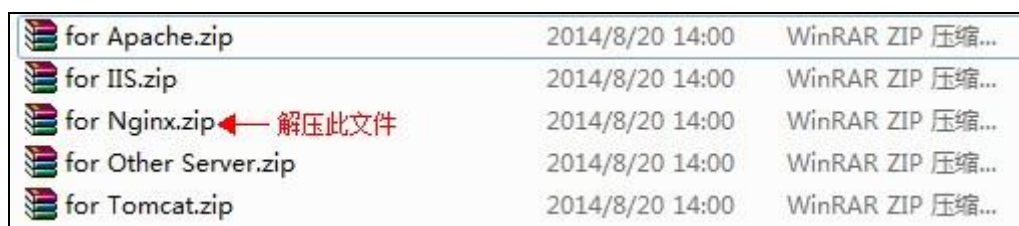


图 1

2.2 解压证书文件

打开 **for Nginx** 文件可以看到 2 个文件。包括公钥、私钥, 如图 1



图 2

2.3 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;
    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:!eNULL;
    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>

三、SSL 证书的备份

请保存好收到的证书压缩包文件及密码，以防丢失

四、SSL 证书的恢复

重复 2.3 操作即可。