Nginx SSL 证书申请部署指南

沃通电子认证服务有限公司

WoSignCA Limited

目　　录

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、 生成证书请求文件

2.1 生成 csr 请求文件

首先下载 openssl 软件，可以去 openssl 官网下载：http://www.openssl.org/related/binaries.html 下载后安装到本地计算机。

2.1.1 查看 openssl

在终端输入 openssl version 查看 openssl 当前版本。

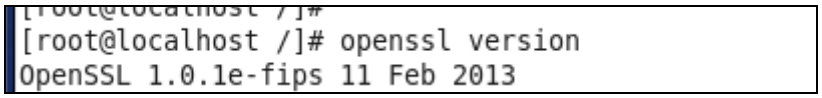

图 1

2.1.2 生成 key 私钥文件

使用以下命令来生成私钥：openssl genrsa -des3 -out www.mydomain.com.key 2048，生成的私钥保存在当前目录。

```
[root@localhost /]# openssl genrsa -des3 -out www.mydomain.com.key 2048
Generating RSA private key, 2048 bit long modulus
..................+++
..............................+++
e is 65537 (0x10001)
Enter pass phrase for www.mydomain.com.key:
Verifying - Enter pass phrase for www.mydomain.com.key:
[root@localhost /]# ls
123.txt  dev   lib         media  proc  selinux  tmp  www.mydomain.com.key
bin      etc   lib64       mnt    root  srv      usr
boot     home  lost+found  opt    sbin  sys      var
[root@localhost /]#
```

图 2

2.1.3 生成 csr 文件

使用以下命令来生成私钥：**openssl req -new -key www.mydomain.com.key -out www.mydomain.com.csr**

```
[root@localhost /]# openssl req -new -key www.mydomain.com.key -out www.mydomain
.com.csr
Enter pass phrase for www.mydomain.com.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:GuangDong
Locality Name (eg, city) [Default City]:ShenZhen
Organization Name (eg, company) [Default Company Ltd]:Wosign CA Limited
Organizational Unit Name (eg, section) []:Wosign Support
Common Name (eg, your name or your server's hostname) []:www.wosign.com
Email Address []:support@wosign.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
[root@localhost /]#
```

图 3

Country Name (2 letter code) [GB]：输入国家地区代码，如中国的 CN
State or Province Name (full name) [Berkshire]：地区省份
Locality Name (eg, city) [Newbury]：城市名称
Organization Name (eg, company) [My Company Ltd]：公司名称
Organizational Unit Name (eg, section) []：部门名称
Common Name (eg, your name or your server’s hostname) []：申请证书域名
Email Address []：电子邮箱
随后可能会提示输入密码，一般无需输入，直接回车即可

三、 提交 CSR 文件

3.1 登录 wosign 站点

登录 https://login.wosign.com/；输入密码和验证码，选择客户端证书登录在线购买系统。

3.2 选择证书类型

点右上边橙色“申请证书”连接，选择您要申请的 SSL 证书，点“立即申请”，

3.3 填写资料

需要填写：证书绑定的域名，申请年限，是否需要发票，并设置证书安装密码。

3.4 验证域名邮箱

进入域名验证，可以选择邮箱验证、DNS 验证或者网站验证方式，进入下一步；

3.5 确认订单信息

用记事本打开生成好的 csr 文件，提交生成的 csr 文件，然后确认订单信息。

3.6 支付订单

可您以在线转账，也可以选择线下转账

3.7 上传证明材料

根据要求上传材料

3.8 等待证书签发

证书申请提交成功。待客服和鉴证审核，您可以联系您的客服专员咨询订单审核情况。

四、 安装 SSL 证书

4.1 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。

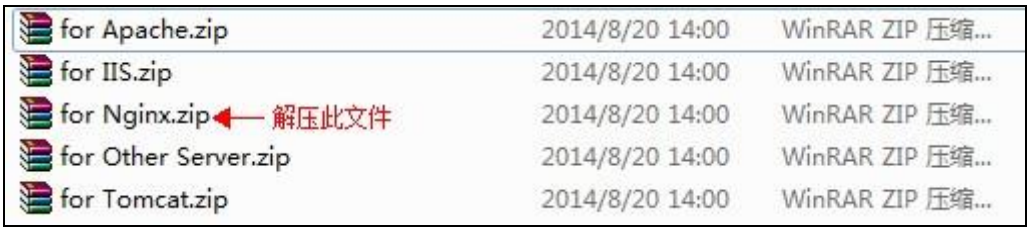

图 5

4. 2 解压证书文件

打开 for Nginx 文件可以看到 1 个文件。证书的公钥，如图 6

图 6

4.3 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_bundle.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

五、 SSL 证书的备份

请保存好收到的证书压缩包文件和证书私钥及密码，以防丢失

六、 SSL 证书的恢复

重复第四步操作即可。