Nginx

二〇二一年一月

目 录

服务器证书安装配置指南（Nginx）

1. 生成证书请求

1.1 安装OpenSSL 工具

您需要使用Openssl 工具来创建证书请求。

下载OpenSSL：http://www.globalsign.cn/Openssl/openssl-1.0.2p.tar.gz

1.2 生成服务器证书私钥

安装OpenSSL 到C:\OpenSSL

命令行进入C:\OpenSSL\bin，运行如下命令：

openssl genrsa -out server.key 2048

该命令执行后将会生成server.key 私钥文件

您还可以选择下载CSR 自动创建程序，快速创建证书请求。

1.3 生成服务器证书请求文件

运行如下命令生成证书请求文件（CSR）：

openssl req -new -key server.key -out certreq.csr

接下来提示输入申请证书的详细信息：

```
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) []:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) []:Shanghai
Organization Name (eg, company) []:GlobalSign China Co., Ltd.

Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your websites domain name) []:cn.globalsign.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

从Email 地址开始，下面的信息都不需要，请保留为空，直接回车即可。

需要输入的信息说明请见下表：

字段	说明	示例
Country Name	ISO 国家代码（两位字符）	CN
State or Province Name	所在省份	Shanghai
Locality Name	所在城市	Shanghai
Organization Name	公司名称	GlobalSign China Co., Ltd.
Organizational Unit Name	部门名称	IT Dept.
Common Name	申请证书的域名	cn.globalsign.com
Email Address	不需要输入	
A challenge password	不需要输入	

完成以上的操作后会在对应的目录下生成server.key 和server.csr，请妥善保存这两个文件。

1.4 备份私钥并提交证书请求

请妥善保存证书私钥文件server.key ， 并将证书请求文件certreq.csr 提交给GlobalSign。

2. 安装服务器证书

2.1 获取服务器证书文件

将证书签发邮件中的包含服务器证书代码的文本复制出来（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到记事本等文本编辑器中。

为保障服务器证书在 IE7 以下客户端的兼容性， 服务器证书需要安装中级CA 证书。中级CA证书包含（中级证书，交叉证书（重要））

在服务器证书代码文本结尾，回车换行，并分别粘贴两张中级 CA 证书代码（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”，每串证书代码之间均使用回车换行分隔），修改文件扩展名，保存为server.cer 文件。 如下图

```
-----BEGIN CERTIFICATE-----
MIIF1DCCBLygAwIBAgIMWboINHBhhjfwJ18XMA0GCSqGSIb3DQEBCwUAMFMxCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSkwJwYDVQQDEyBH
（服务器证书，此处内容已省略.....）
P1MWfEuOdKxPKmZeCj+njr8HjL2QFJP1AtQhie9svkV0h95IyTDVfy2MOHEj1wv/
GnaDvs8MGuCtivSQhD33tJ2ibfnaHd6PBA8tOCfQZeRcEOteRV5fWixITC9vel9b
G2sGfTTxYXk=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEsDCCA5igAwIBAgIQd70OB0LV2enQSdd00CpvmjANBgkqhkiG9w0BAQsFADBM
MSAwHgYDVQQLExdHbG9iYWxTaWduIFJvb3QgQ0EgLSBSMzETMBEGA1UEChMKR2xv
（中级证书，此处内容已省略.....）
XRrLOD1kS1hyBjsfyTNZrmL1h117IFgntBA5SQNV19ckedq5r4RSAU85jV8XK5UL
REjRZt2I6M9Po9QL7guFLu4sPFJpwR1sPJvubS2THeo7SxYoNDtdyBHs7euaGcMa
D/fayQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIETjCCAzagAwIBAgINAe5fFp3/lzUrZGXWajANBgkqhkiG9w0BAQsFADBXMQsw
CQYDVQQGEwJCRTEZMBcGA1UEChMQR2xvYmFsU2lnbiBudi1zYTEQMA4GA1UECxMH
（交叉证书，此处内容已省略.....）
WOx37XMiwor1hkOIreoTbv3Y/kIvuX1erRjvlJDKPSerJpSZdcfL03v3ykzTr1Eh
kluEfSufFT90y1HonoMOFm8b50bOI7355KKL0jlrqnkckSziYSQtjipIcJDEHsXo
4HA=
-----END CERTIFICATE-----
```

2.2 安装服务器证书

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

```
# HTTPS server
#
#server {
# listen 443;
# server_name localhost;
# ssl no;
# ssl_certificate etc/ssl/server.cer
# ssl_certificate_key etc/ssl/server.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

```
server {
listen 443;
server_name localhost;
ssl on;
ssl_certificate etc/ssl/server.cer;
ssl_certificate_key etc/ssl/server.key;
ssl_session_timeout 5m;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH;
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。

3. 服务器证书的备份与恢复

在您成功的安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您的系统应用带来不便。

3.1 服务器证书的备份

备份服务器证书私钥文件 server.key，以及服务器证书文件 server.cer 即可完成服务器证书的备份操作。

3.2 服务器证书的恢复

请参照服务器证书配置部分，将服务器证书密钥文件恢复到您的服务器上，并修改配置文件，恢复服务器证书的应用。

请注意，此文档会不定期更新！

GlobalSign China Co., Ltd

环玺信息科技（上海）有限公司

2021年 1 月