



服务器证书安装配置指南

Apache for Linux

二〇二一年一月

目录

1. 安装准备.....	2
1.1 安装Openssl.....	2
1.2 安装Apache.....	2
2. 生成证书请求文件.....	2
2.1 创建私钥.....	2
2.2 生成证书请求 (CSR) 文件.....	2
2.3 备份私钥并提交证书请求文件.....	3
3. 安装服务器和中级CA证书.....	3
3.1 获取CA 证书.....	3
3.2 获取服务器证书.....	3
Apache 2.0.63 的配置.....	4
Apache 2.2.* 的配置.....	4
4. 服务器证书的备份及恢复.....	5
4.1 服务器证书的备份.....	5
4.2 服务器证书的恢复.....	5

1. 安装准备

1.1 安装Openssl

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 安装Apache

```
./configure --prefix=/usr/local/apache --enable-so --enable-ssl --with-ssl=/usr/local/ssl --  
enable-mods-shared=all //配置安装。推荐动态编译模块
```

```
make && make install
```

动态编译Apache 模块，便于模块的加载管理。Apache 将被安装到/usr/local/apache

2. 生成证书请求文件

2.1 创建私钥

在创建证书请求之前，您需要首先生成服务器证书私钥文件 server.key。

```
cd /usr/local/ssl/bin //进入openssl 安装目录
```

```
openssl genrsa -out server.key 2048 // 运行openssl 命令，生成2048 位长的私钥
```

server.key 文件。如果您需要对server.key 添加保护密码，请使用-des3 扩展命令。

Windows 环境下不支持加密格式私钥，Linux 环境下使用加密格式私钥时，每次重启Apache都需要您输入该私钥密码（例：openssl genrsa -des3 -out server.key 2048）。

2.2 生成证书请求（CSR）文件

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

Country Name : //您所在国家的ISO 标准代号，中国为CN

State or Province Name : //您单位所在地省/自治区/直辖市

Locality Name : //您单位所在地的市/县/区

Organization Name : //您单位/机构/企业合法的名称

Organizational Unit Name : //部门名称

Common Name : //通用名，例如：cn.globalsign.com。此项必须与访问提供 SSL 服务的服务器时所应用的域名完全匹配。

Email Address : //您的邮件地址，不必输入，直接回车跳过

"extra" attributes : //以下信息不必输入，回车跳过直到命令执行完毕。

2.3 备份私钥并提交证书请求

请将证书请求文件certreq.csr 提交给GlobalSign，并备份保存证书私钥文件server.key，等待证书的签发。服务器证书密钥对必须配对使用，私钥文件丢失将导致证书不可用。

3. 安装服务器证书

3.1 获取CA证书

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 CA 证书（CA证书包含中级证书，交叉证书（重要））。从邮件中获取 CA证书：

将证书签发邮件中的从 BEGIN 到 END 结束的两段 CA证书内容（包括 “-----BEGIN CERTIFICATE-----” 和 “-----ENDCERTIFICATE -----”）粘贴到同一个记事本等文本编辑器中。修改文件扩展名，保存为 intermediate.cer 文件。如下

```

-----1-----2-----3-----4-----5-----6-----7-----
1  -----BEGIN CERTIFICATE-----
2  MIIETjCCAzagAwIBAgINAe5fIh38YjvUMzqFVzANBgkqhkiG9w0BAQsFADBMMSAw
3  （中级证书，此部分内容省略.....）
4  hriSqHKvof1Shx8xpfywgVcvzfT03PYkz6f1NJBonf6q8amaEsybwMbDqKwwIX7e
5  SPY=
6  -----END CERTIFICATE-----
7  -----BEGIN CERTIFICATE-----
8  MIIETjCCAzagAwIBAgINAe5fFp3/1zUrZGXWajANBgkqhkiG9w0BAQsFADBXMQsw
9  （交叉证书，此部分内容省略.....）
10 kluEfSufFT90y1HonoMOfm8b50b0I7355KkL0j1rqnkckSziYSQtjipIcJDEHsXo
11 4HA=
12 -----END CERTIFICATE-----|
13
14
15
16
17
18
19

```

3.2 获取服务器证书

将证书签发邮件中的从BEGIN 到END 结束的服务器证书内容（包括 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----”）粘贴到记事本等文本编辑器中，保存为 server.cer 文件，如图

```

-----1-----2-----3-----4-----5-----6-----7-----
1  -----BEGIN CERTIFICATE-----
2  MIIGvjCCBaagAwIBAgIMfNwsGF9vGSWvy66oMA0GCSqGSIb3DQEBCwUAMFAxCzAJ
3  （服务器证书，此部分内容省略.....）
4  NSH3m8dEsQzhHmdK8bGA6vsCQHJ4+XIRTJT6Ew2ncYT9maq3ndJ8h6zGffsXqDRN
5  UpY=
6  -----END CERTIFICATE-----|

```

Apache 2.0.63 的配置

打开 Apache 安装目录下 conf 目录中的httpd.conf 文件，找到：

```
#LoadModule ssl_module modules/mod_ssl.so
```

删除行首的配置语句注释符号“#”保存退出。

打开 apache 安装目录下 conf 目录中的 ssl.conf 文件，找到在配置文件中查找以下配置语句：

```
SSLCertificateFile conf/server.cer    将服务器证书配置到该路径下
```

```
SSLCertificateKeyFile conf/server.key  将服务器证书私钥配置到该路径下
```

```
SSLCertificateChainFile conf/intermediate.cer
```

删除行首的“#”号注释符，并将 CA证书 intermediate.cer 配置到该路径下

保存退出，并重启 Apache。

通过https 方式访问您的站点，测试站点证书的安装配置。

Apache 2.2.* 的配置

打开 apache 安装目录下 conf 目录中的 httpd.conf 文件，找到：

```
#LoadModule ssl_module modules/mod_ssl.so
```

```
#Includeconf/extra/httpd_ssl.conf
```

删除行首的配置语句注释符号“#”保存退出。

打开 apache 安装目录下 conf/extra 目录中的httpd-ssl.conf 文件，在配置文件中查找以下配置语句：

```
SSLCertificateFile conf/ssl.crt/server.cer 将服务器证书配置到该路径下
```

```
SSLCertificateKeyFile conf/ssl.key/server.key 将服务器证书私钥配置到该路径下
```

```
#SSLCertificateChainFile conf/ssl.crt/intermediate.cer
```

删除行首的“#”号注释符，并将CA证书intermediate.cer配置到该路径下

保存退出，并重启 Apache。

通过https 方式访问您的站点，测试站点证书的安装配置。

4. 服务器证书的备份及恢复

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

4.1 服务器证书的备份

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

4.2 服务器证书的恢复

请参照服务器证书配置部分，将服务器证书和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，此文件会不定期更新！

GlobalSign China Co., Ltd

环玺信息科技（上海）有限公司

2021年 1 月