



## 服务器证书安装配置指南

### Apache for Linux

Q/GlobalSign China-QI-XX-YY

GlobalSign 数字证书颁发机构  
环玺信息科技（上海）有限公司

2018 年 1 月

## 目 录

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

## 1. 安装准备

### 1.1 安装 Openssl

要使 Apache 支持 SSL, 需要首先安装 Openssl 支持。推荐下载安装 openssl-0.9.8k.tar.gz  
 下载 Openssl: <http://www.openssl.org/source/>

```
tar -zxf openssl-0.9.8k.tar.gz //解压安装包
cd openssl-0.9.8k //进入已经解压的安装包
./config //配置安装。推荐使用默认配置
make && make install //编译及安装
openssl 默认将被安装到/usr/local/ssl
```

### 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。

```
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: www.itrus.com.cn。此项必须与您访问提供 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 获取服务器证书中级 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两张中级 CA 证书。

从邮件中获取中级 CA 证书:

将证书签发邮件中的从 BEGIN 到 END 结束的两张中级 CA 证书内容 (包括 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----”) 粘贴到同一个记事本等文本编辑器中, 中间用回车换行分隔。修改文件扩展名, 保存为 intermediatebundle.crt 文件。

### 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.crt 文件

#### 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/ssl.crt/server.crt
```

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

下

```
#SSLCertificateChainFile conf/ssl.crt/ca.crt
```

删除行首的 “#” 号注释符, 并

将中级 CA 证书 intermediatebundle.crt 配置到该路径下

保存退出，并重启 Apache。重启方式：

进入 Apache 安装目录下的 bin 目录，运行如下命令

```
./apachectl -k -stop
./apachectl startssl
```

## 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
#Include conf/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.crt
SSLCertificateKeyFile conf/ssl.key/server.key
#SSLCertificateChainFile conf/ssl.crt/ca.crt
级 CA 证书 intermediatebundle.crt 配置到该路径下
```

将服务器证书配置到该路径下

将服务器证书私钥配置到该路径下

删除行首的“#”号注释符，并将中

保存退出，并重启 Apache。重启方式：

进入 Apache 安装目录下的 bin 目录，运行如下命令

```
./apachectl -k -stop
./apachectl startssl
```

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.crt，以及服务器证书中级 CA 证书文件 intermediatebundle.crt 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。