Apache SSL 服务器证书部署指南

修订日期：2017/12/12

目 录

一、 部署前特别说明

1. GDCA 信鉴易® SSL 服务器证书部署指南(以下简称“本部署指南”)主要描述如何通过 GDCA 在线系统产生密钥对证书部署到 Apache 服务器

2. 本部署指南适用于 linux、windows 系统下 Apache 2.x 版本；

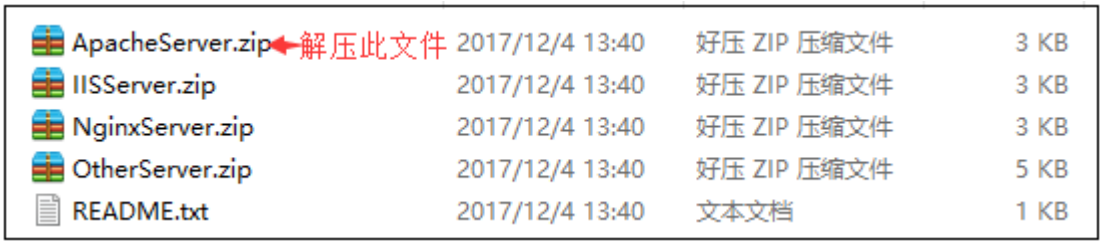
3. Apache 服务器部署恒信企业 EV SSL 和睿信 SSL 证书的操作步骤一致，区别在于：前者在 IE7 以上浏览器访问时，浏览器会显示安全锁标志，地址栏会变成绿色；而后者在浏览器访问时，浏览器显示安全锁标志，但地址栏不会变成绿色。

4.本部署指南使用 testweb.95105813.cn 作为样例进行安装配置，实际部署过程请用户根据正式的域名进行配置。

二、 获取服务器证书

1. 获取证书文件

在您完成申请数安时代 GDCA 服务器证书的流程后，登录系统将会下载一个压缩文件,使用里面的 ApacheServer.zip 文件:



解压之后获得证书如下图：

2. 获取私钥文件

请找到之前提交 csr 时生成的.key 私钥文件，该文件为证书的私钥，请找到此文件，后面配置要用到此文件；

三、 安装服务器证书

1. 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

(如果找不到请确认是否编译过 OpenSSL 插件)

#Include conf/extra/httpd_ssl.conf 删除行首的配置语句注释符号“#” 保存退出。

2. 打开 apache 安装目录下 conf/extra 目录中的 httpd-ssl.conf 文件

3. 打开 Apache2.x/conf/extra/目录下的 httpd-ssl.conf 文件,将

ServerName www.example.com:443 改成您的主机域名,

DocumentRoot 指定网页文件路径;(此处的配置和 http 的 80 端口配置文件保持一致)

4.修改 SSL 协议支持语句，关闭不安全的协议和加密套件

SSLProtocol all -SSLv2 -SSLv3

5.修改加密套件如下

SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!3DES:!MD5:!ADH:!RC4:!DH:!DHE

6.找到如下三个选项 SSLCertificateFile、SSLCertificateKeyFile 和 SSLCertificateChainFile 这三个配置项，将 testweb.95105813.cn.crt 和 tetweb.95105813.cn.key 及证书链 issuer.crt 文件上传到指定目录下（这里是/usr/local/apache/conf/sslcert，windows 路径也可以自己指定）

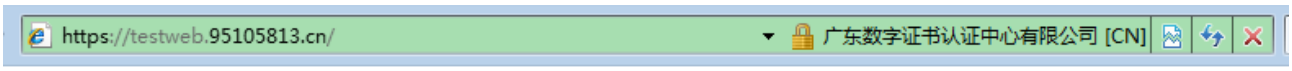
完整的配置文件如下：

```
<VirtualHost *:443>
ServerName       www.domain.com:443              #网站域名
DocumentRoot    "/usr/local/apache/www"           #网站主目录
SSLEngine on
SSLProtocol    all -SSLv2 -SSLv3
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!3DES:!MD5:!ADH:!RC4:!DH:!DHE
SSLCertificateFile       "/usr/local/apache/conf/sslcert/testweb.95105813.cn.crt"
SSLCertificateKeyFile     "/usr/local/apache/conf/sslcert/testweb.95105813.cn.key"
SSLCertificateChainFile    "/usr/local/apache/conf/sslcert/issuer.crt"
</VirtualHost>
```

7.保存退出，并重启 Apache

四、 访问测试

服务器若部署了 SSL 证书，浏览器访问时将出现安全锁标志；若部署了 EV SSL 证书，IE 浏览器除了显示安全锁标志，地址栏会变成绿色，（如果访问不通，请查看服务器防火墙是否拦截 443 端口）如下图：



五、 备份和恢复

在您完成服务器证书的安装与配置后，请务必要备份好您的服务器证书，避免证书遗失给您造成不便

1. 备份服务器证书

备份好证书压缩文件及证书私钥.key 的文件。

2. 恢复服务器证书

参照步骤“三、安装服务器证书”即可完成恢复操作。

六、 证书遗失处理

若您的证书文件损坏或者丢失且没有证书的备份文件，请联系 GDCA（客服热线 95105813）办理遗失补办业务，重新签发服务器证书。