

# 网站安装ssli证书(http转https)

2017年12月08日 10:17:42 小键666 阅读数: 4934 标签: https SSL 更多

版权声明：本文为博主原创文章，未经博主允许不得转载。 https://blog.csdn.net/qq\_37214710/article/details/78748176

环境lamp Apache2.4版本(其他版本自行测试)






申请SSL证书 本人在数安时代申请的 链接https://www.trustauth.cn/

并不是只有数安时代SSL证书可以使用 其他网站的也可以 自行申请

## 一、获取SSL证书

### 1. 获取证书文件

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;

 ApacheServer.zip	解压此文件	2017/12/4 13:40	好压 ZIP 压缩文件	3 KB
 IISServer.zip		2017/12/4 13:40	好压 ZIP 压缩文件	3 KB
 NginxServer.zip		2017/12/4 13:40	好压 ZIP 压缩文件	3 KB
 OtherServer.zip		2017/12/4 13:40	好压 ZIP 压缩文件	5 KB
 README.txt		2017/12/4 13:40	文本文档	1 KB

解压之后获得证书如下图:

名称	修改日期	类型
 issuer.crt	2017/12/4 13:40	安全证书
 testweb.95105813.cn.crt	2017/12/4 13:40	安全证书

## 二、安装服务器证书

### 1.修改httpd.conf文件

打开apache安装目录下conf目录中的httpd.conf文件,路径如: /usr/local/apache/conf/httpd.conf，找到以下两项去掉前面的#注释，保存并退出。

(如果找不到请确认是否编译过 OpenSSL 插件)

```
1 LoadModule ssl_module modules/mod_ssl.so
2 Include conf/extra/httpd-ssl.conf
```

### 2.修改主机域名

打开Apache2.x/conf/extra/目录下的httpd-ssl.conf文件，修改如下语句：

```
ServerName www.*****.com:443 #您的网站域名
```

### 3.添加SSL协议支持语句，关闭不安全的协议和加密套件

```
SSLProtocol all -SSLv2 -SSLv3
```

### 4.修改加密套件如下:

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

### 5.添加证书配置语句:

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 及中级证书issuer.crt文件上传到服务器目录（可以自己建一个文件夹放进去 这里是/usr/local/apache/conf/sslcert，windows路径自己指定）

完整的配置文件如下:

```
1 <VirtualHost *:443>
2     ServerName      www.domain.com:443           #网站域名
3     DocumentRoot    "/usr/local/apache/www"       #网站主目录和80端口配置保持一致
4     SSLEngine on
5     SSLProtocol     all -SSLv2 -SSLv3
6     SSLCipherSuite  ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!3DES:!ADH:!RC4:!DH
7     SSLCertificateFile  "/usr/local/apache/conf/sslcert/testweb.95105813.cn.crt" #证书公钥
8     SSLCertificateKeyFile  "/usr/local/apache/conf/sslcert/testweb.95105813.cn.key" #证书私钥
9     SSLCertificateChainFile  "/usr/local/apache/conf/sslcert/issuer.crt" #中级证书
10 </VirtualHost>
```

### 6.重启Apache

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

如果访问不通 进行如下步骤(可以访问的可跳过本步骤):

在阿里云添加安全组 操作步骤如下:

1. 登录 云服务器管理控制台。
2. 单击左侧导航中的 安全组。
3. 选择地域。
4. 找到要授权规则的安全组，单击 配置规则。
5. 单击 添加安全组规则。
6. 在弹出的对话框中，设置下面参数:

添加安全组规则

网卡类型：

内网

规则方向：

入方向

授权策略：

允许

协议类型：

HTTPS (443)

\* 端口范围：

443/443

优先级：

1

授权类型：

安全组访问

☒ 本账号授权 ☐ 跨账号授权

授权对象：

请选择安全组

描述：

长度为2-256个字符，不能以http://或https://开头。

确定

取消

该步骤设置完成后 95% 都可用https访问 如果还是访问不通 可能是你的配置文件有问题 重新配置一下

## HTTP自动跳转到HTTPS步骤:

在你网站目录下放一个.htaccess文件。windows环境下，不能把文件直接改名为.htaccess，会提示你必须输入文件名。所以我们先新建一个“新建文本文档.txt”文档，记事本打开，选择另存为，保存类型选择“所有文件(\*.\*)”，文件名输入“.htaccess”，保存。这样便生成了一个.htaccess文件。

编辑器打开.htaccess文件，写入如下规则:

```
1 <IfModule mod_rewrite.c>
2     RewriteEngine On
3     RewriteCond %{HTTPS} !=on
4     RewriteRule ^(.*) https://%{SERVER_NAME}/$1 [R,L]
5 </IfModule>
```

这样便实现了输入网址直接跳转到https下