# 服务器证书安装配置指南（Apache）

## 一、Linux 系统 https 配置流程

说明：
域名： www.domain.com
操作系统： Centos 7.6 （64 位）
Apache 版本： 2.4.6

### 1、确认 mod_ssl.so 模块是否安装

首先打开 apache 配置文件，确认是否安装 mod_ssl.so 模块,由于 apache 各个版本的配置略有不同，mod_ssl.so 所在位置也不同。基本在以下两个文件中：

```
/etc/httpd/conf/httpd.conf
/etc/httpd/conf.modules.d/00-ssl.conf
```

分别编辑两个文件：

```
#  vi  /etc/httpd/conf/httpd.conf
#  vi  /etc/httpd/conf.modules.d/00-ssl.conf
```

查看是否有下边三行，如果有注释 # 的话把 # 删除。

```
LoadModule ssl_module modules/mod_ssl.so
Include conf.modules.d/*.conf
IncludeOptional conf.d/*.conf
```

默认的 apache 安装是不安装 mod_ssl.so 模块的，需要我们通过 yum 方式安装。

```
#   yum install -y   mod_ssl
```

安装完后/etc/httpd/conf.d 目录下会出现一个 ssl.conf 文件（/etc/httpd/conf/httpd.conf 文件中需要 IncludeOptional conf.d/*.conf 或者 Include conf.d/*.conf ，ssl.conf 的配置才生效）。

### 2、ssl.conf 基本配置

```
# vi   /etc/httpd/conf.d/ssl.conf
```

主要关注以下几行：

```
SSLEngine on
SSLProtocol -all +TLSv1.3 +TLSv1.2
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM
SSLHonorCipherOrder on
SSLCertificateFile /etc/httpd/conf.d/server.crt
SSLCertificateKeyFile /etc/httpd/conf.d/server.key
SSLCertificateChainFile /etc/httpd/conf.d /CA.crt
```

证书的位置为 /etc/httpd/conf.d,也可以放在其他位置，记得修改路径。

## 3、测试配置是否正确

使用命令 services httpd configtest 或者 apachectl configtest 测试一下配置是否存在错误，没有错误 ok。

```
# apachectl configtest
[root@localhost conf.d]# apachectl configtest
Syntax OK
```

测试没有问题，重启 httpd 服务器

```
# service httpd force-reload
[root@localhost ~]# service httpd force-reload
Redirecting to /bin/systemctl force-reload  httpd.service
```

## 4、访问 http 直接跳转 https

在实际使用中，多数访问 http 的访问被重定向到 https,就需要在 http 的配置增加如下红色文字的内容：

```
#    vi /etc/httpd/conf.d/http-vhost.conf
```

```
<VirtualHost *:80>
    ServerAdmin admin@domain.com
    DocumentRoot "/var/www/html"
    ServerName      www.domain.com

    RewriteEngine on
    RewriteCond     %{HTTPS} !=on
    RewriteRule     ^(.*)    https://%{SERVER_NAME}$1 [L,R]

    DirectoryIndex index.htm
```

```
    ErrorLog "/var/log/httpd/error_log"
    CustomLog "/var/log/httpd/access_log" combined
    <Directory "/var/www/html">
        Options -Indexes +FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

保存配置文件后，测试配置是否正确，然后重启 httpd 服务器使配置生效。

## 5、谷歌浏览器输入框显示不正确说明

如果 https 配置正确，显示如下图，在 https 前面会有一把锁。


鼠标点击锁会显示如下图的结果：


如果 https 配置正确，但在浏览器的输入框中 https 前面显示的不是一把锁而是如下图显示：


点击这个小图标显示如下图：证书（有效），但显示您与此网站之间建立的链接并非完全安

全


解决办法：

当用 https://www.domain.com 访问时，在 apache 站点默认索引文件 index.html (或者 index.htm、index.php 等等)调用了 http 方法，文件包含 http://www.domain.com/news/xx.html 等等，需要将此类的 http://www.domain.com/ 修改为 https://www.domain.com/。

如果网页中有友情链接之类的外部链接不用修改。

# 二、Windows 系统 https 配置流程

说明：
域名： www.domain.com
操作系统： Windows server 2008 （64 位）
Apache 版本： 2.4

## 1、准备工作：

下载并安装 Apache windows 版本自带 openssl 的安装包。

Apache 官网只提供源码，用户可以自行编译。推荐使用 xampp 这类在 windows 平台有更加友好操作界面的控制平台，其中内附了 apache、mysql 等常用的服务器必备软件，一键安装省去了调试和配置的麻烦。

安装好 apache 后，打开 apache 安装目录，以 C:\xampp\apache 为例。打开目录下的 bin 目录，确认其中是否有 openssl.exe，如果有，说明此 apache 是包含 openssl 的，无需再装 openssl。从网上的资料来看，现在还没有独立安装好 apache 后再安装 openssl 并使其协调

工作的完美解决方案，所以一定要在安装 apache 时就确认其已经包含了 openssl。

数字证书保存位置：C:\xampp\Apache\conf\cert\，你也可以放在自定义的目录下。

## 2、开启 Apache 的 SSL 功能：

打开 httpd.conf，在 C:\xampp\apache\conf\目录下。
删除下面两行前面的注释 # 符号，并保存

#LoadModule ssl_module modules/mod_ssl.so
#Include conf/extra/httpd-ssl.conf

打开 C:\xampp\Apache\conf\extra\httpd-ssl.conf 文件，修改 httpd-ssl.conf 文件，保存退出
在..\Apache\conf\extra 目录下，打开 httpd-ssl.conf 文件（注：先备份一份，以免出错.）
在文件中定位到 Listen 443 这行，把从这行到这个文件结尾的文本全部注释掉或者删除掉，替换成以下代码。

```
Listen 443
SSLStrictSNIVHostCheck off
SSLCipherSuite  EECDH+AESGCM:EDH+AESGCM
SSLProtocol   -all +TLSv1.3 +TLSv1.2
<VirtualHost *:443>
    #这里的路径设置你的网站根目录
    DocumentRoot "C:\xampp\Apache\htdocs"

    #这里 domain.com 替换成你的域名
    ServerName www.domian.com

    #这里 domain.com 替换成你的域名
    ServerAlias domain.com

    #这里的路径设置你的网站根目录
    <Directory "C:\xampp\Apache\htdocs">
        Options FollowSymLinks ExecCGI
        AllowOverride All
        Order allow,deny
        Allow from all
        Require all granted
    </Directory>
    SSLEngine on

    #你的公钥文件
    SSLCertificateFile "C:/xampp/Apache/conf/cert/server.crt"
```

```
    #你的私钥文件
     SSLCertificateKeyFile "C:/xampp/Apache/conf/cert/server.key"

     #证书链文件（有的签发机构命名为 CA.crt）
     SSLCertificateChainFile "C:/xampp/Apache/conf/cert/CA.crt"
</VirtualHost>
```

重启 apache 服务，看看 apache 服务能不能正常启动，启动浏览器检查是否可以访问 https://localhost 及 https://www.domain.com，如果有异常，尝试把 httpd-ssl.conf 代码恢复注释（把#重新加上去，保存退出或者用备份文件覆盖），再次重启 apache，如果此时能够正常启动，则说明 httpd-ssl.conf 文件中配置有错误，（是不是 443 端口被占用重复监听了？证书路径对不对？是不是路径少双引号？证书是否有效？），请认真检查，直到能够正常启动 apache 服务。

## 三、防火墙开放 443 端口

https 配置完成后，在本机访问没有问题，但外部网络访问 https 网页时却打不开，就需要确认防火墙是否把 443 端口对外开放了。Linux 和 Windows 本身的防火墙(iptables、firewalld、windows 防火墙)以及对外出口总的防火墙都需要检查。

## 四、多域名多证书配置

示例配置：

```
Listen 443
NameVirtualHost *:443
#  第一个虚拟主机
<VirtualHost *:443>
DocumentRoot "/var/www/html"
ServerName www.AAA.com
SSLEngine on
SSLCertificateFile /etc/httpd/ssl/AAAserver.crt
SSLCertificateKeyFile /etc/httpd/ssl/AAAserver.key
SSLCertificateChainFile /etc/httpd/ssl/CA.crt
</VirtualHost>

#第二个虚拟主机
<VirtualHost *:443>
DocumentRoot "/var/www/html"
```

```
ServerName www.BBB.com
SSLEngine on
SSLCertificateFile /etc/httpd/ssl/BBBserver.crt
SSLCertificateKeyFile /etc/httpd/ssl/BBBserver.key
SSLCertificateChainFile /etc/httpd/ssl/CA.crt
</VirtualHost>
```