

Copyright 2021 By Sectigochina All Right Reserved.

# Guide for SSL Installation in Apache v2.2

Apache v2.2 安装配置SSL证书方法教程



## Apache v2.2 安装配置SSL证书方法教程

- ① SSL证书安装配置
- ② 检查SSL证书配置
- ③ 使用SSL加密通信示例
- ④ SSL配置说明和安装过程中的常见错误信息

成功获取SSL证书之后，下载到本地的是一个压缩文件，解压后里面包含pem后缀文件是证书文件，\_chain.crt后缀是证书链(中间证书)文件，Root.crt后缀文件是根证书文件。

## Apache v2.2 安装配置SSL证书方法教程

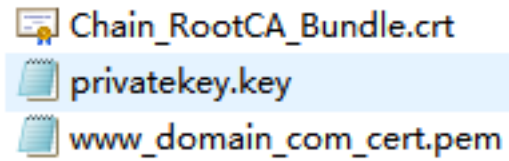
### SSL证书安装配置(根据证书类型说明)

•单域名，多域名和通配符SSL证书安装之间的差异

产品	不同点
单域名	如果您在单个服务器上安装两个以上的证书，则单域名证书无法共享一个端口。但是，它可以通过 <a href="#">Apache 2.2.12版本</a> 中的SNI函数来共享端口。
多域名	由于多域名证书能够 <b>共享端口</b> ，添加NameVirtualHost设置， <code>&lt; Virtual Host&gt; ~ &lt;/ Virtual Host&gt;***</code> 按照域名数量设置即可。 其他步骤与文中所述相同
通配符	由于通配符域证书能够使用 <b>所有子域并共享端口</b> ，因此添加NameVirtualHost的配置，并根据要安装的域设置 <code>&lt;Virtual Host&gt; ~ &lt;/ Virtual Host&gt;</code> 的元素。 其他步骤与文件中所述相同

## SSL证书安装

- 1、解压下载的证书文件压缩包
- 2、解压下载的key文件压缩包
- 3、解压后将如下三个文件移动到服务器上, 路径为: apache/conf/ssl /



证书文件：以.pem为后缀或文件类型。  
证书链文件：以.crt为后缀或文件类型。  
密钥文件：以.key为后缀或文件类型。



## SSL证书安装配置

### • 1. 修改Apache配置文件(httpd.conf)

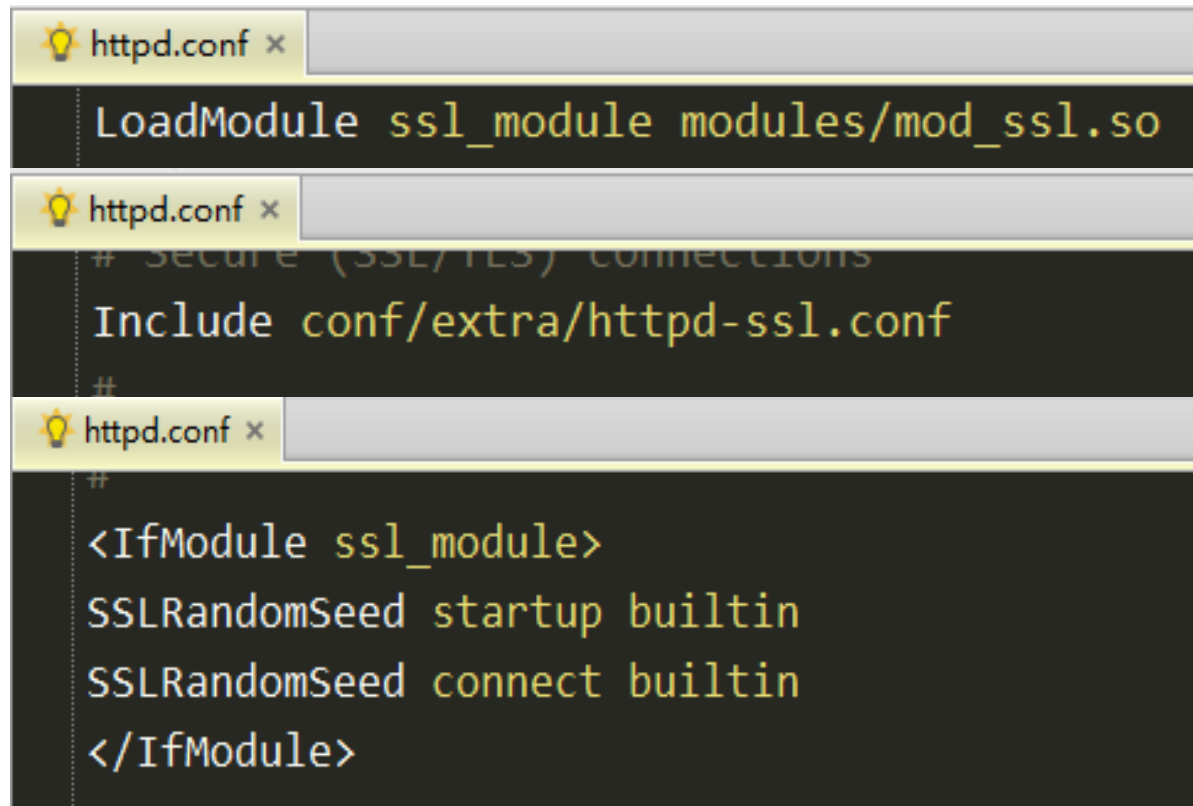
- **httpd.conf** : 通常, 此配置文件位于以下 apache/conf 文件夹中

(1) "LoadModule ssl\_module modules/mod\_ssl.so" 行中检查是否已删除注释项 (Sharp代码: "#")

(2) "Include conf / extra / httpd-ssl.conf" 行中检查是否已删除注释 (Sharp代码: "#")。

(3) <IfModule ssl\_module> ~ </ IfModule> 行中检查是否已删除注释 (Sharp代码: "#")。

说明: 如果您在httpd.conf文件中没有找到以上配置语句, 请确认您的Apache服务器中是否已经安装mod\_ssl.so模块。可执行 yum install -y mod\_ssl 命令安装 mode\_ssl 模块。



```
httpd.conf x
LoadModule ssl_module modules/mod_ssl.so

httpd.conf x
# secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#

httpd.conf x
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
```



## SSL 证书安装配置

- 2 修改Apache SSL配置文件(httpd-ssl.conf)
  - httpd-ssl.conf :通常该配置文件位于 “ apache/con/extra” 文件夹中

说明： 根据操作系统的不同， http-ssl.conf文件也可能存放在conf.d/ssl.conf目录中。

```
<VirtualHost *:443>
  DocumentRoot "/data/www/www.domain.com/" #与httpd.conf配置相同的目录
  ServerName "www.domain.com" #Web服务器的域名
  ServerAdmin "admin.domain.com"
  ErrorLog "/www/server/apache/logs/error_log"
  TransferLog "/www/server/apache/logs/access_log"
  SSLEngine on
  SSLCertificateFile "/www/server/apache/conf/ssl/www_domain_com.pem" #路径/证书文件名
  SSLCertificateKeyFile "/www/server/apache/conf/ssl/privatekey.key" #路径/私钥文件名
  SSLCertificateChainFile "/www/server/apache/conf/ssl/Chain_RootCA_Bundle.crt" #路径/证书链文件名
</VirtualHost>
```

#如果证书包含多个域名，复制以上参数，并将ServerName替换成第二个域名。

```
<VirtualHost *:443>
  DocumentRoot "/data/www/www.domain2.com/" #与httpd.conf配置相同的目录
  ServerName "www.domain2.com" #Web服务器的域名
  ServerAdmin "admin.domain2.com"
  ErrorLog "/www/server/apache/logs/error_log"
  TransferLog "/www/server/apache/logs/access_log"
  SSLEngine on
  SSLCertificateFile "/www/server/apache/conf/ssl/www_domain2_com.pem" #路径/证书文件名
  SSLCertificateKeyFile "/www/server/apache/conf/ssl/privatekey.key" #路径/私钥文件名
  SSLCertificateChainFile "/www/server/apache/conf/ssl/Chain_RootCA_Bundle.crt" #路径/证书链文件名
</VirtualHost>
```



## SSL 证书安装配置

- 3. 可选: 修改httpd.conf文件, 设置HTTP请求自动跳转HTTPS。

在httpd.conf文件中的<VirtualHost \*:80> </VirtualHost>中间, 添加以下重定向代码。

```
RewriteEngine on  
RewriteCond %{SERVER_PORT} !^443$  
RewriteRule ^(.*)$ https://%{SERVER_NAME}$1 [L,R]
```

- 4. 重启Apache服务器使SSL配置生效

(1) 停止Apache服务。

```
apachectl -k stop
```

(2) 开启Apache服务。

```
apachectl -k start
```

### SSL证书安装检查

- 完成Apache SSL配置后重新启动Apache Web服务器(httpd-ssl.conf).
  - 在重新启动Web服务器的过程中发生错误时, 请检查SSL错误日志(ssl\_error\_log) 还有SSL访问错误日志 (ssl\_access\_log)
  - 连接到 “ https: // [applied\_domain]: port” , 通过单击浏览器地址窗口右侧的锁定图标, 检查HTTPS通信。



\*证书安装完成后, 如果网站无法通过https正常访问, 需确认您安装证书的服务器443端口是否已开启或被其他工具拦截。

**如果与网络服务器的连接仍然不可用, 请参阅本指南中的“SSL配置说明和安装过程中的常见错误信息”**

## SSL配置说明和安装过程中的常见错误信息

- “如果证书和私钥不匹配，则证书将无法正确加载。”
  - **申请发行证书时，只能使用生成CSR的私钥的证书。**
    - 如果申请过程中多次生成私钥，则只能使用在最终申请时CSR生成的私钥。
- “私钥与颁发的SSL证书不匹配时的错误消息和日志”
  - **日志/显示匹配的错误消息，例如“密钥和证书不匹配” ‘Matching Error’**
    - 例) “私钥和SSL证书不匹配” (Keyword: Matching)
      - >使用在CSR创建的私钥文件重新配置，否则您必须请求再次申请证书颁发。
  - **记录/显示链错误消息，例如“中间（链）验证失败”。**
    - 例) “无法验证中间证书链” (Keyword: Chain)
      - >检查中间证书（链）的配置
        - 1)对于需要导入的Web服务器（例如密钥库），请检查是否导入了中间证书。
        - 2)对于单独设置中间证书路径的Web服务器，请检查中间证书路径和文件位置。
  - **显示与“Password Error”相关的错误消息日志**
    - 例) “私钥中的密码与您输入的密码不同” (Keyword: Private Key, Password, Passphrase)
      - >重新颁发证书，因为密码与您输入的密码不同。(caused by file error or password error)
- “有关在单个服务器上使用多域的说明”
  - HTTPS (SSL) 的端口不能重复或共享。
    - 通常，在单个服务器上安装两个证书需要两个不同的端口。但是，使用“通配符证书”或“多域名证书”可以共享端口。
- **‘通配符SSL证书(\*.sectigochina.com)’ 和 ‘多域名SSL证书’ 是可端口共享的SSL证书。**
  - 在安装多域证书后，向证书申请增加其他域名时，必须重新安装证书。



## SSL配置说明和安装过程中的常见错误信息

- 当HTTPS端口未设置为“443”而是其他端口时，则在输入URL时也应包括该端口。
  - [https://.com:443]由于端口号“443”是为SSL端口保留的，因此可以省略。
  - [https:// www.sectigochina.com:8443]打算将其设置为SSL端口时，应在URL末尾注明端口号“8443”。  
**-本文档中使用的端口号是一个示例(Can be changed)**
- 加载错误的SSL证书（未安装到Web服务器中）时，HTTPS连接会发生错误。
  - **访问已安装的Web服务器并检查已加载的证书**
    - > 在访问https: // [Web服务器IP地址]: 端口时显示的错误消息上，单击“继续访问此网站（不推荐）”。
    - 检查Web浏览器中加载的SSL证书信息。如果显示已安装的证书，则需要检查是否需要将SSL证书安装到L4，防火墙或Web服务器前面的任何其他设备中。**
- **Android v5.0 (Lollipop) +或Google Chrome浏览器无法连接到https时**
  - **更改选项以在SSL协议中使用TLSv1.2和TLSv1.1，并更新Web服务器中最新的补丁程序以确保安全。**
    - > 因为2014年底SSLv3协议中发现了安全漏洞，如果Web服务器不支持比TLSv1.1更新的推荐协议，则该Web服务器的访问权限可能不可用。
- **HTTPS连接延迟和证书吊销列表（CRL）警告消息**
  - **如果它不是公共网络，并且对外部CRL或OCSP URL的网络访问受到限制，则可能会因浏览器无法搜索SSL证书信息而发生错误异常**
    - > 需要通过打开防火墙等网络设备中的相关URL（或IP地址）和端口，使用户能够顺利连接到外部网络。
    - （由于CRL，OCSP URL根据颁发的证书而不同，因此需要在“证书属性”的“详细信息”选项卡中找到“CRL分发点”和“授权信息访问”的URL信息。**

## SSL配置说明和安装过程中的常见错误信息

- “当用户访问目标域时，出现“已颁发证书无效”错误消息。
  - **适用于封闭网络等特定环境中的用户。**
    - >当Web服务器没有将中间证书交付给用户（连接到Web服务器）时，就会发生这种情况，因为Web服务器在中间证书的安装中存在问题。
      - 在这种情况下，请再次检查本指南文档中的中间证书安装部分。
  - **对于使用WINDOWS XP，Internet Explorer 8或更低版本，或未将WINDOWS O / S更新为最新的用户。**
    - >当用户（连接到网络服务器）环境中不存在根证书时，就会发生这种情况。
      - 在这种情况下，请使用“控制面板”中的“Windows Update”更新WINDOWS O / S软件，或将随附的RootCA.crt文件手动安装到用户计算机（用户PC）。
- 用户访问目标域时，出现“Web服务器的SSL证书已过期”错误消息。
  - **检查用户PC（连接到Web服务器）中的系统时间是否与Internet时间服务器同步。**
  - **在“[证书属性]”的“[详细信息]”选项卡中检查SSL证书的到期日期。**
    - >即使域证书已更新，当再次发生相同错误时，也需要检查是否需要将SSL证书安装到L4，防火墙或Web服务器前面的其他设备中。
- “用户访问目标域时，出现“网络服务器的SSL证书被吊销”错误消息
  - **请致电Sectigochina进行有关过期和已撤销证书的查询。**



**THANK YOU**