Apache 服务器安装 SSL 证书

环玺信息科技（上海）有限公司

GlobalSign China Co., Ltd

目 录

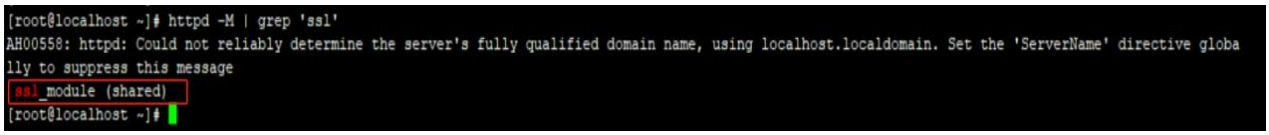
本文将全面介绍如何在 Apache 服务器配置 SSL 证书，具体包括在 Apache 上配置证书文件、证书链和证书密钥等参数，以及安装证书后结果的验证。成功配置 SSL 证书后，您将能够通过 HTTPS 加密通道安全访问 Apache 服务器。

重要：本文以 CentOS 7.9 64 位操作系统、Apache 2.4.6 为例介绍。不同版本的操作系统或 Web 服务器，部署操作可能有所差异。

前提条件

拥有证书，若您没有证书，请联系您购买证书时所对应的销售人员进行咨询。

- **证书文件（CER 格式）**
- **证书链文件（CER 格式）**
- **私钥文件（KEY 格式）**
- **Apache 服务器已安装 mod_ssl.so 模块（启用 SSL 功能）**
- **如未安装，可执行 yum install -y mod_ssl 命令安装。安装后，可执行 httpd -M | grep 'ssl' 检查 mod_ssl.so 是否安装成功。安装成功效果图：**



步骤一：在 Apache 服务器安装证书

1. 执行以下命令，在 Apahce 的安装目录下创建一个用于存放证书的 cert 目录

①. 进入 Apache 的安装目录

```
cd /etc/httpd/  #使用 yum 安装 Apache 的默认安装目录。如果您手动修改过该目录或使用其他方式安装的 Apache，请根据实际配置调整
```

②. 创建 cert 目录

```
mkdir cert  #创建证书目录，命名为 cert
```

2. 将证书文件、证书链文件和私钥文件上传到 Apache 服务器的证书目录（/etc/httpd/cert）

3. 编辑 Apache 配置文件 httpd.conf 和 ssl.conf，修改与证书相关的配置

①. 找到 LoadModule ssl_module modules/mod_ssl.so（用于加载 mod_ssl.so 模块启用 SSL 服务）和 Include conf.modules.d/*.conf（用于加载 SSL 配置目录），并检查是否被注释，如果被注释，请删除#注释

> **重要** 由于操作系统以及Apache安装方式不同，以上文件所处的位置也不同。可能出现在Apache目录的以下位置：
>
> - **conf.modules.d/00-ssl.conf**：本文中 `LoadModule ssl_module modules/mod_ssl.so` 位于该配置文件下。
> - **httpd.conf**：本文中 `Include conf.modules.d/*.conf` 位于该配置文件下。
> - **http-ssl.conf**
>
> 如果仍未找到以上参数，请确认您的Apache服务器中是否已经安装mod_ssl.so模块。如未安装，可执行 `yum install -y mod_ssl` 命令安装，安装后，可执行 `httpd -M | grep 'ssl'` 命令检查mod_ssl.so是否安装成功。

②. 执行以下命令，打开 ssl.conf 配置文件

```
vim /etc/httpd/conf.d/ssl.conf
```

> **重要** ssl.conf文件在不同操作系统的位置和名称不一样，在没有ssl.conf文件的情况下，请您查看Apache安装目录是否存在conf/extra/http-ssl.conf配置文件。

③. 在 ssl.conf 配置文件中，定位到以下参数，按照文中注释修改

```
<VirtualHost *:443>
 #修改为申请证书时绑定的域名。
 ServerName yourdomain:443
 #将 yourdomain.cer 替换成您证书文件名。
 SSLCertificateFile cert/yourdomain.cer
 #将 yourdomain.key 替换成您证书的密钥文件名。
 SSLCertificateKeyFile cert/yourdomain.key
 #将 yourdomain_chain.cer 替换成您证书的证书链文件名。
 SSLCertificateChainFile cert/yourdomain_chain.cer
</VirtualHost>
```

```
#如果证书包含多个域名，复制 VirtualHost 参数，并将 ServerName 修改为第二个域名。
<VirtualHost *:443>
 #修改为申请证书时绑定的第二个域名。
 ServerName yourdomain:443
 #将 yourdomain2 替换成您申请证书时的第二个域名。
 SSLCertificateFile cert/yourdomain2.cer
 #将 yourdomain2 替换成您申请证书时的第二个域名。
 SSLCertificateKeyFile cert/yourdomain2.key
 #将 yourdomain2 替换成您申请证书时的第二个域名。
 SSLCertificateChainFile cert/yourdomain2_chain.cer
</VirtualHost>
```

重要 请关注您的浏览器版本是否支持SNI功能。如果不支持，多域名证书配置将无法生效。

④. 可选：修改 conf/httpd.conf 文件，设置 HTTP 请求自动跳转 HTTPS

在 httpd.conf 文件中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. 启动 apache 服务：`systemctl start httpd`

②. 停止 apache 服务：`systemctl stop httpd`

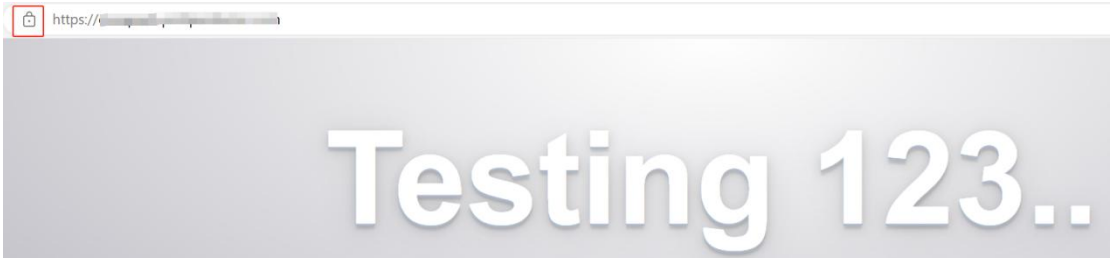
③. 重启 apache 服务：`systemctl restart httpd`

步骤二：验证 SSL 证书是否安装成功

证书安装完成后，您可通过访问证书的绑定域名验证该证书是否安装成功。

```
https://yourdomain    #需要将 yourdomain 替换成证书绑定的域名
```

如果网页地址栏出现小锁标志，表示证书已经安装成功。



技术支持邮箱地址:support-china@globalsign.com

文档支持站点地址:https://www.globalsign.cn/resources/installation