

国密 SM2 证书 Apache 安装指南-Linux



沃通电子认证服务有限公司

WoTrus CA Limited

目录

一、 环境准备	2
二、 安装证书	3
三、 检测 SSL 配置	7
四、 备份 SSL 证书	7

技术支持邮箱: supp3@wotrus.com

技术支持热线电话: 18822828659 / 0755-26027827

公司官网地址: <https://www.wotrus.com>

一、环境准备

目前仅支持 Linux 环境下 Apache;

- 1、Linux 操作系统(仅支持 X86_64 架构);
- 2、Apache 下载链接:<http://httpd.apache.org/download.cgi>;
- 3、国密 SM2 模块(根据系统版本, 提供 V1 和 V2 两种版本国密模块, 以 Centos 为例)

Centos 6 及以下版本: https://www.wotrus.com/download/wotrus_ssl_v1.tar.gz;

Centos 7 及以上版本: https://www.wotrus.com/download/wotrus_ssl.tar.gz;

- 4、沃通国密 SM2 、RSA SSL 证书;

二、安装证书

- 1、安装 Apache(文档以 [apache-2.4.46](#) 为例, 目录为/usr/local, 用户根据实际环境操作即可);

安装 apache 之前, 先安装相关的依赖库, 如果系统是全新的, 请先安装 gcc/gcc-c++:

```
yum install -y gcc yum install -y gcc-c++;
```

- (1)、安装 apr: <https://dlcdn.apache.org/apr/apr-1.7.4.tar.gz>, 下载并上传 apr-1.7.4.tar.gz 至/usr/local 目录下:

解压: `tar -zxvf apr-1.7.4.tar.gz`

检测: `cd apr-1.7.4`

`./configure --prefix=/usr/local/apr`

编译: `make && make install`

- (2)、安装 apr-util: <http://archive.apache.org/dist/apr/apr-util-1.5.4.tar.gz>, 下载并上传至/usr/local 目录下: (推荐使用 apr-util-1.5 的版本, 1.6 的兼容性有问题)

解压: `tar -zxvf apr-util-1.5.4.tar.gz`

检测: `cd apr-util-1.5.4`

```
./configure --prefix=/usr/local/apr-util --with-apr=/usr/local/apr
```

编译: `make && make install`

Ps:make 时如果出现`#include <expat.h> ^ compilation terminated.`的报错, 请 `yum install -y expat-devel` 安装依赖库。

(3)、安装 pcre: 连网状态下, 可执行命令 `yum install -y pcre-devel` 或者通过 <https://sourceforge.net/projects/pcre/files/pcre/8.45/pcre-8.45.tar.gz/download> 下载并上传至 `/usr/local` 目录下:

解压: `tar -zxvf pcre-8.45.tar.gz`

检测: `cd pcre-8.45`

```
./configure --prefix=/usr/local/pcre
```

编译: `make && make install`

(4)、上述三个文件编译安装完成后, 将下载的 apache 国密版和国密模块也上传至 `/usr/local` 目录下:

解压: `tar -zxvf wotrus_ssl.tar.gz`

`mv wotrus_ssl wotrus_ssl2.0.4(以 2.0.4 为例)`

`tar -zxvf apache-2.4.46.tar.gz`

检测: `cd apache-2.4.46`

```
./configure --prefix=/usr/local/httpd --enable-so --enable-ssl
```

```
--enable-cgi --enable-rewrite --enable-modules=most --enable-mpms-shared=all
```

```
--with-mpm=prefork --with-zlib --with-apr=/usr/local/apr
```

```
--with-apr-util=/usr/local/apr-util --with-ssl=/usr/local/wotrus_ssl
```

Ps:以上只编译了部分模块, 如有需求, 请用户自行添加需要的模块

编译: `make`

`make install`

Ps:上述步骤中的目录皆是测试环境的目录, 具体路径, 请根据实际用户环境!

2、配置 SSL

(1)、申请证书后，下载得到 domain.com_sm2.zip 的压缩包，解压后会得到如下三个文件夹：

名称	修改日期	类型
test.wosign.com_rsa	2024/2/26 14:04	文件夹
test.wosign.com_sm2_encrypt	2024/2/26 14:04	文件夹
test.wosign.com_sm2_sign	2024/2/26 14:04	文件夹

Apache 上需要用到三个文件夹下 NginxServer 中.crt 文件和申请证书创建 CSR 时保存的两个.key 文件；

(2)、上传 SSL 证书，cd 进入/usr/local/httpd/conf，新建 cert 目录，将上面解压的 crt 文件以及创建 CSR 时生成的两个.key 文件(分别是 rsa 和 sm2 命名的 key 文件)上传至该目录；

(3)、配置 SSL 证书，进入/usr/local/httpd/conf，vi/vim 编辑 httpd.conf 文件，找到 **#LoadModule ssl_module modules/mod_ssl.so**，去掉前面的注释符#，增加 **Include conf/ssl.conf**，保存退出后在/usr/local/httpd/conf，vi/vim 新建一个 ssl.conf 文件，增加如下配置：

```
Listen 443

<VirtualHost *:443>

    ServerName  domain.com

    DocumentRoot  website 根目录

    SSLEngine on

    #RSA config

    SSLCertificateFile  /usr/local/httpd/conf/domain.com_bundle.crt

    SSLCertificateKeyFile  /usr/local/httpd/conf/domain.com_rsa.key

    #SM2 sign config

    SSLCertificateFile  /usr/local/httpd/conf/domain.com_sm2_sign_bundle.crt
```

```
SSLCertificateKeyFile    /usr/local/httpd/conf/domain.com_sm2.key  
  
#SM2 encrypt config  
  
SSLCertificateFile      /usr/local/httpd/conf/domain.com_sm2_encrypt_bundle.crt  
  
SSLCertificateKeyFile    /usr/local/httpd/conf/domain.com_sm2.key  
  
#sign 和 encrypt 配置中的.key 和 bundle.crt 为同一个  
  
SSLProtocol all -SSLv2 -SSLv3  
  
SSLCipherSuite  
  
ECC-SM4-SM3:ECDH:AESGCM:HIGH:MEDIUM:!RC4:!DH:!MD5:!aNULL:!eNULL  
  
SSLHonorCipherOrder on  
  
<Directory "website 根目录">  
  
    Options -Indexes -FollowSymLinks +ExecCGI  
  
    AllowOverride None  
  
    Order allow,deny  
  
    Allow from all  
  
    Require all granted  
  
</Directory>  
</VirtualHost>
```

以上仅为参考(http 的配置请自行处理), 具体的 **ServerName**, 证书名称, 证书目录, **Directory** 等配置请根据实际环境配置!

(4)、检测: `/usr/local/httpd/bin/httpd -t`,若提示 Syntax OK, 则表示配置正常, 可以启动 apache。

如果有提示错误, 请根据提示排查错误, 直到显示正常!

(5)、启动: 执行 `/usr/local/httpd/bin/httpd -k start`, 启动 apache!

三、检测 SSL 配置

下载沃通密信浏览器测试 https 访问，下载地址：

https://download.wosign.com/wosign/MeSignBrowser_setup.exe

下载安装后，打开浏览器，在地址栏输入 <https://domain.com>(证书实际绑定域名)测试是否能正常访问以及显示国密字样，如无法正常访问，请确保防火墙或安全组等策略有放行 443 端口（SSL 配置端口）。

四、备份 SSL 证书

请将下载的.zip 压缩包和自主生成的私钥.key 文件备份，以防丢失，影响后续使用！