国密 SM2 证书 Nginx 安装指南

沃通电子认证服务有限公司

WoTrus CA Limited

目录

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

1、Linux 操作系统(目前仅支持 X86_64 架构)；

2、Nginx -1.14.2 及以上版本（推荐使用**最新稳定版**），附下载链接:http://nginx.org/en/download.html；

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 Nginx**(文档以 nginx-1.15.12 为例，目录为/usr/local，用户根据实际环境操作即可)；

在安装 nginx 前，需要确保系统安装了 gcc-c++、pcre-devel 和 zlib-devel 软件。

(1) 、将上述步骤下载的 nginx 压缩包和 wotrus_ssl.tar.gz，上传至 linux 操作系统/usr/local/目录下，分别解压；

(2) 、cd 进入 nginx 的解压目录 usr/local/nginx-1.15.12，执行./configure

--prefix=/usr/local/nginx --with-http_stub_status_module --with-stream

--with-http_ssl_module --with-stream_ssl_module

--with-openssl=/usr/local/wotrus_ssl

Ps:这里只指定了几个需要的模块，其他模块用户可自行增加；

(3)、上述步骤执行完成后，再输入 make && make install，编译 nginx。执行该步骤后，若无报错，则表示编译成功，可以开始配置证书；如果执行过程中出现

```
make[1]: *** [/usr/local/wotrus_ssl//.openssl/include/openssl/ssl.h] 错误 127
make: *** [build] Error 2
```

如上图显示的错误，则需要进入 nginx-1.15.12/auto/lib/openssl 目录，

vi/vim 编辑 conf 文件(可先备份)，找到下面所示的四行代码：

CORE_INCS="$CORE_INCS $OPENSSL/.openssl/include"

CORE_DEPS="$CORE_DEPS $OPENSSL/.openssl/include/openssl/ssl.h"

CORE_LIBS="$CORE_LIBS $OPENSSL/.openssl/lib/libssl.a"

CORE_LIBS="$CORE_LIBS $OPENSSL/.openssl/lib/libcrypto.a"

改为:

CORE_INCS="$CORE_INCS $OPENSSL/include"

CORE_DEPS="$CORE_DEPS $OPENSSL/include/openssl/ssl.h"

CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libssl.a"

CORE_LIBS="$CORE_LIBS $OPENSSL/lib/libcrypto.a"

保存后，先执行 make clean,再重新执行(2)步骤的./configure 和(3)步骤的 make && make install;

(4)、编译完成后，cd 进入/usr/local/nginx 目录，用 /usr/local/nginx/sbin/nginx -t 检测是否正常，正常则输入 /usr/local/nginx/sbin/nginx 启动 nginx;

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)、下载 SSL 证书，解压下载的 domain.com_sm2.zip 压缩包，解压后会得到以下文件：

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

Nginx 配置需要用到三个文件夹中 NginxServer 中的.crt 文件，私钥文件为申请证书创建 CSR 时保存的两个.key 文件(sign 和 encrypt 可共用同一个私钥)。

(2)、上传 SSL 证书，cd 进入/usr/local/nginx/conf，新建 sm2 目录，将上面的三个

crt 文件以及两个.key 文件上传至该目录；

(3)、配置 SSL 证书，进入/usr/local/nginx/conf，vi/vim 编辑 nginx.conf 文件，增加如下配置，然后保存:

```
server {
        listen          443 ssl;
        server_name  domain.com;
        ssl_certificate     /usr/local/nginx/conf/sm2/domain.com_rsa.crt;
        ssl_certificate_key     /usr/local/nginx/conf/sm2/domain.com_rsa.key;

        ssl_certificate     /usr/local/nginx/conf/sm2/domain.com_sign.crt;
        ssl_certificate_key     /usr/local/nginx/conf/sm2/domain.com_sm2.key;

        ssl_certificate     /usr/local/nginx/conf/sm2/domain.com_en.crt;
        ssl_certificate_key     /usr/local/nginx/conf/sm2/domain.com_sm2.key;
        #先配置签名证书，再配置加密证书，签名加密证书私钥 key 为同一个！
        ssl_session_timeout    5m;
        ssl_protocols    TLSv1.1 TLSv1.2 TLSv1.3;
        ssl_ciphers
ECC-SM4-SM3:ECDH:AESGCM:HIGH:MEDIUM:!RC4:!DH:!MD5:!aNULL:!eNULL;
        ssl_prefer_server_ciphers       on;

        location / {
            root     html;
            index    index.html index.htm;
        }
    }
```

以上仅为参考，具体的 server_name，证书名称，证书存放目录，location 等配置请根据实际环境配置！

(4)、检测，执行/usr/local/nginx/sbin/nginx -t，看配置是否正常，正常显示如下图:

```
[root@localhost nginx-1.15.12]# /usr/local/nginx/sbin/nginx -t
Use GM signing certificate.
Use GM signing private key.
Use GM encryption certificate.
Use GM decryption private key.
nginx: the configuration file /usr/local/nginx/conf/nginx.conf syntax is ok
nginx: configuration file /usr/local/nginx/conf/nginx.conf test is successful
```

如果有提示错误，请根据提示排查错误，直到显示正常！

(5)、重启 nginx：执行/usr/local/nginx/sbin/nginx -s reload，重启 nginx！

三、检测 SSL 配置

下载沃通密信浏览器测试国密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！