国密算法 Web 环境改造及 RSA/SM2 双算法证书部署帮助文档

在部署支持国密算法的 SSL 证书时，为了确保与各类浏览器的兼容性，通常会采用 SM2/RSA 双证书部署方案，即您需要在服务器同时配置国际通用的 RSA 算法证书和国密标准的 SM2 算法证书。本文档为您介绍在 Linux 系统下，如何使用 Tengine+Tongsuo 组合方式，实现 Tengine 服务器双算法证书部署。

背景信息

Tengine：是一款开源、高性能、可扩展的 Web 服务器和反向代理服务器，它在 Nginx 的基础上，针对大访问量网站的需求，添加了很多高级功能和特性。更多关于 Tengine 的说明，请参见 Tengine 官网（https://tengine.taobao.org/）。

Tongsuo：是一个提供现代密码学算法和安全通信协议的开源基础密码库，如需了解更多，请参见铜锁密码库官网（https://www.tongsuo.net/）。

安装所使用的命令包

在服务器执行以下命令安装需要使用的软件命令包

```
yum -y install wget
yum -y install gcc  gcc-c++
yum -y install make
yum -y install pcre  pcre-devel
yum -y install gzip
yum -y install zlib-devel
```

安装 Tongsuo 和 Tengine

1、下载 Tongsuo 并解压

```
wget -c https://www.joyssl.com/Nginx_SM2_download/Tongsuo-8.2.1.tar.gz
tar -zxvf Tongsuo-8.2.1.tar.gz
```

2、下载 Tengine 并解压

```
wget -c https://www.joyssl.com/Nginx_SM2_download/tengine-2.4.1.tar.gz
tar -zxvf tengine-2.4.1.tar.gz
```

3、进入 Tengine 解压目录

```
cd /root/tengine-2.4.1/
```

4、在 Tengine 解压目录下，执行以下命令，编译安装 Tengine 并关联 Tongsuo

```
./configure --prefix=/usr/local/tengine  \
--add-module=modules/ngx_tongsuo_ntls  \
--with-openssl=../Tongsuo-8.2.1  \
--with-openssl-opt="enable-ntls"  \
--with-http_ssl_module  \
--with-stream \
--with-stream_ssl_module \
--with-stream_sni
make -j
make install
```

部署证书

1、执行以下命令在 Tengine 服务器配置文件目录中创建证书存放目录

```
cd /usr/local/tengine/conf
mkdir cert #创建证书目录，命名为 cert
```

2、将证书相关文件上传到 cert 目录（示例位于/usr/local/tengine/conf/cert）

Lunix 系统可使用 FTP 客户端工具，通过 SFTP over SSH 上传

3、编辑 Tengine 配置文件 nginx.conf（示例文件位于/usr/local/tengine/conf），修改 SSL 相关配置：

```
server {
    listen 443 ssl;
    server_name joyssl.com;    # 修改为对应的网站域名
    enable_ntls on; # 启用 NTLS。

    # 配置国密算法签名证书
    ssl_sign_certificate cert/server_sign.pem;    # 修改为实际证书文件路径
    ssl_sign_certificate_key cert/server_sign.key;    # 修改为实际私钥文件路径

    # 配置国密算法加密证书
    ssl_enc_certificate cert/server_enc.pem;    # 修改为实际证书文件路径
    ssl_enc_certificate_key cert/server_enc.key;  # 修改为实际私钥文件路径

    # 配置 RSA 算法证书
    ssl_certificate cert/server_rsa.pem;    # 修改为实际证书文件路径
    ssl_certificate_key cert/server_rsa.key;  # 修改为实际私钥文件路径

    ssl_session_cache shared:SSL:1m;
    ssl_session_timeout 5m;

    # 配置加密套件
    ssl_ciphers ECC-SM2-SM4-CBC-SM3:ECC-SM2-SM4-GCM-SM3:ECDHE-SM2-SM4-CBC-SM3:ECDHE-SM2-SM4-GCM-SM3:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-SHA256:!aNULL:!eNULL:!RC4:!EXPORT:!DES:!3DES:!MD5:!DSS:!PKS;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
    ssl_prefer_server_ciphers on;

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

4、执行如下命令，重启 Tengine 服务

```
cd /usr/local/tengine/sbin # 进入 Tengine 服务的可执行目录
./nginx -s reload  # 重新载入配置文件
```

5、验证是否成功

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。

SM2 算法证书验证需使用国密浏览器测试，常用国密浏览器有零信、红莲花、赢达信、360 国密等。

RSA 算法证书使用 Google、Firefox、Edge 等浏览器测试。

常见问题及解决方案

在编辑 nginx.conf 配置文件之后，执行命令无法重启 Tengine 服务，并出现下面报错:

```
open() "/usr/local/tengine/logs/nginx.pid" failed (2: No such file or directory)
```

```
invalid PID number "" in "/usr/local/tengine/logs/nginx.pid"
```

是因为每一个 nginx 进程都对应一个 id，存放于 nginx.pid 中，可能在系统编译时出现 bug，导致 nginx.pid 创建失败或 id 出错，服务无法重启。可按照如下方法解决:

```
cd /usr/local/tengine/sbin  # 进入 Tengine 服务的可执行目录
killall -9 nginx  # 杀掉所有 nginx 进程
./nginx -t  #检查配置文件是否有错
./nginx  # 启动 nginx
./nginx -s reload  # 重载配置文件，测试
```