



链滴

Linux 版 Tomcat 证书一键生成脚本

作者: [tlbcc](#)

原文链接: <https://ld246.com/article/1611251336203>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

使用JRE中的keytool工具生成Tomcat可以使用的SSL2048位PKCS12格式自签证书。

脚本使用方式，如果脚本名为 `ssl.sh`，使用方式如下：

```
./ssh.sh 365
```

需要传入证书有效天数，作为参数。

脚本内容如下：

```
#!/bin/sh
# SSL证书生成

# 证书有效期（单位天）
VALIDITY_DAY=$1
JAVA_BIN_HOME="/root/jdk1.8.0_271/bin"
SSL_HOME="/root/test/javassl"

rm ${SSL_HOME}/* -rf
# 1. 生成服务端keystore
${JAVA_BIN_HOME}/keytool -genkey -keystore "${SSL_HOME}/server.keystore" -alias server -
eyalg RSA -validity $1 -storetype PKCS12 -dname "CN=TLBCC, OU=TLBCC, O=TLBCC, L=beiji
g, ST=beijing, C=cn" -keypass 123456 -storepass 123456

# 2. 验证服务端证书
${JAVA_BIN_HOME}/keytool -list -v -keystore "${SSL_HOME}/server.keystore" -storepass 1234
6

# 3. 导出服务端cer
${JAVA_BIN_HOME}/keytool -export -alias server -keystore "${SSL_HOME}/server.keystore" -rf
-file "${SSL_HOME}/server.cer" -storepass 123456

# 4. 生成truststore，公钥证书导入
${JAVA_BIN_HOME}/keytool -import -alias server -v -file "${SSL_HOME}/server.cer" -keystore
${SSL_HOME}/server.truststore" -storetype PKCS12 -storepass 123456 << EOF
y
EOF

# 5.验证keystore
${JAVA_BIN_HOME}/keytool -list -v -keystore "${SSL_HOME}/server.truststore" -storepass 123
56
```

生成的文件：

- server.keystore - 存放私钥的文件
- server.truststore - 存放可信任的证书文件
- server.cer -证书文件