Tomcat SSL 证书部署指南

沃通电子认证服务有限公司

WoTrus CA Limited

目录

技术支持联系方式

技术支持邮箱：support@wotrus.com

技术支持热线电话：0755-26027828 / 0755-26027859

技术支持网页：https://bbs.wosign.com

公司官网地址：https://www.wosign.com

声明

此文档仅做参考使用，相应的配置需根据当前的配置进行调整。

一、安装 SSL 服务器证书

1.1 获取 SSl 证书

最终沃通数字证书系统将会给您颁发证书文件（.zip）压缩格式，当中有包含三种证书格式如：for Apache、for Ngnix、for Other Server；Tomcat 应用服务器上需要 for Nginx 里面的 crt 证书文件，然后用工具合成 jks 格式：

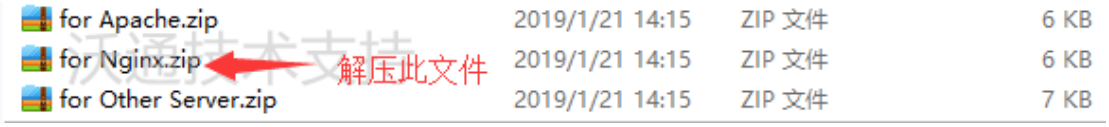


图 1

打开 for Nginx 文件可以看到公钥，如图 2

图 2

私钥 key 文件，需要找到生成 CSR 一起生成出的两个文件，如图 3

图 3

合成工具下载地址：https://download.wosign.com/wosign/wosigncode.exe

合成方式：先把 key 文件放到 for nginx 里，再双击下载的工具，选择证书项，操作选项，选择证书格式转换，源格式选择 PEM，目标格式选择 JKS。

证书文件：点击后面的选择按钮，找到 for nginx 目录，选择 yourdomain.com_bundle.crt，点击确定。

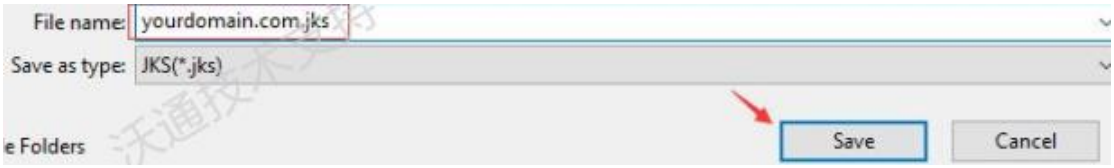
私钥文件：点击后面的选择按钮，找到 for nginx 目录，选择 yourdomain.com.key，点

击确定。

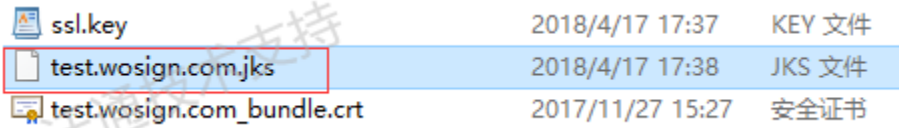
私钥密码：为空，不用填写（因为生成私钥的时候没有填写，如果之前有填写过私钥密码，这里也填写相同的私钥密码）

JKS 密码：任意填写一个密码 （合成 JKS 格式证书后的密码，之后在 tomcat 上安装证书的时候需要使用到）

填写完毕后，点击转换，选择保存证书文件的位置，填写证书名称，推荐使用 yourdomain.com.jks，点击保存。



最后，得到 jks 格式证书。



1.2 部署 SSL 证书

1.2.1 Tomcat 8.5 之前版本

找到 Tomcat 安装目录 conf 下的“Server.xml”，用文本编辑器打开，找到如下图示位置 如图 12：

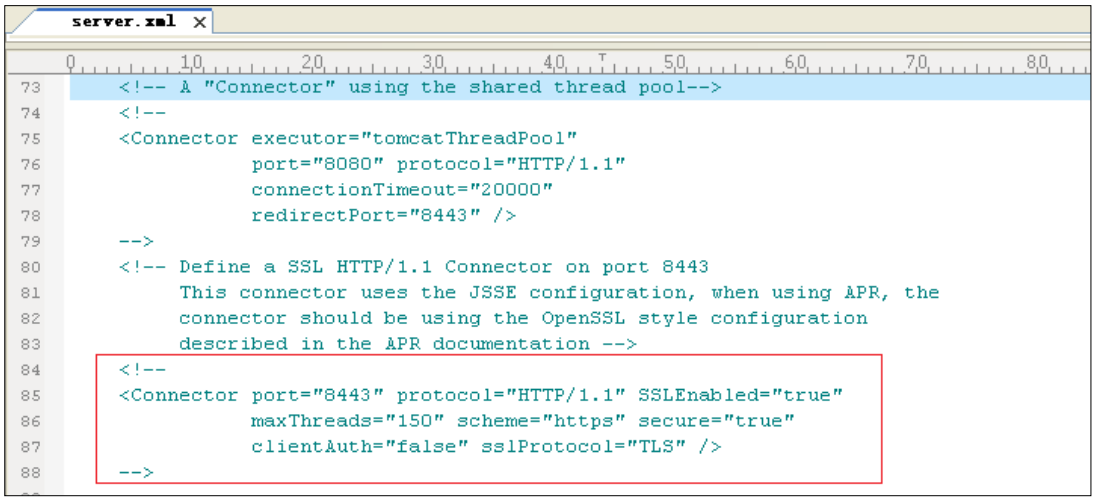


图 12

默认情况下<Connector port=“8443”……>是被注释的，我们可以把“<!-- -->”去掉，然后对其节点进行相应的修改，比如：

配置示例如下：

<Connector port="443" protocol="org.apache.coyote.http11.Http11Protocol"

maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

keystoreFile="keystore/domain.jks" keystorePass="证书密码"

clientAuth="false" sslProtocol="TLS"

ciphers="TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
SSL_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA" />

备注：port：端口号；

keystoreFile：证书路径(例如：**conf/name.jks**)；keystorePass：证书密码。

最后保存该配置文件，然后重启 Tomcat 后再次访问。如图 13：

图 13

1.2.2 Tomcat 8.5 及之后版本

找到 Tomcat 安装目录 conf 下的“Server.xml”，用文本编辑器打开，找到如下图示位

置 如图 14：

```
-->
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
           maxThreads="150" SSLEnabled="true">
    <SSLHostConfig>
        <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"
                     type="RSA" />
    </SSLHostConfig>
</Connector>
-->
```

图 14

默认情况下<Connector port=“8443”……>是被注释的，我们可以把“<!-- -->”去掉，并进行相应的修改。配置示例如下：

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true">
    <SSLHostConfig>
        <Certificate certificateKeystoreFile="F:\Tomcat 9.0\conf\name.jks"
        certificateKeyAlias="1"
        certificateKeystorePassword="证书密码"
        type="RSA" />
    </SSLHostConfig>
</Connector>
```

备注：port：端口号；

certificateKeystoreFile：证书路径(例如：conf/name.jks)；

certificateKeystorePassword：证书密码；

certificateKeyAlias：证书别名

最后保存该配置文件，然后重启 Tomcat 后再次访问即可。如图 5

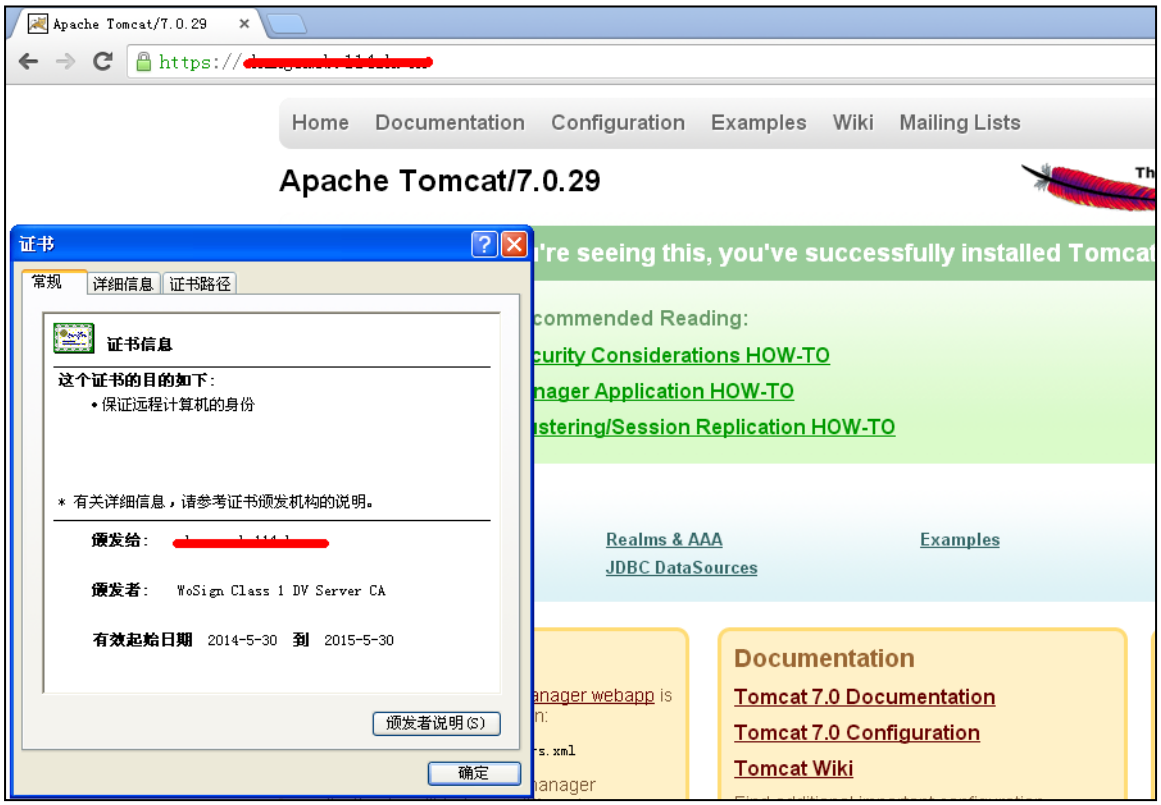


图 5

备注：安装完 ssl 证书后部分服务器可能会有以下错误，请按照链接修复

a. 加密协议和安全套件：https://bbs.wosign.com/thread-1284-1-1.html

b. 部署 https 页面后出现排版错误，或者提示网页有不安全的因素，可参考以下链接：https://bbs.wosign.com/thread-1667-1-1.html

二、SSL 证书的备份

请保存好收到的证书压缩包文件及自己生成 csr 一起的.key 文件，以防丢失

三、SSL 证书的恢复

重复第 1.2 步操作即可。