Tomcat 安装 SSL 证书

操作步骤（本文教程以 Tomcat 7 为例）：

1、解压 Tomcat 证书。

解压后您将看到文件夹中有 2 个文件，您可为两个证书文件重命名。

证书文件（domain name.jks）：以.jks 为后缀或文件类型。

密码文件（password.txt）：以 .txt 为后缀或文件类型。

（ps:如证书格式为 pfx，则需要执行第 2 步，如证书格式为 jks,则跳过第 2 步，从第 3 步开始）

2、如果是 PFX 格式的证书需将 PFX 格式的证书转换成 JKS 格式。

（2.1） 输入以下 JAVA JDK 命令：

```
keytool -importkeystore -srckeystore domain name.pfx -destkeystore domain name.jks -srcstore type PKCS12 -deststoretype JKS
```

说明如果 Windows 系统中，需在%JAVA_HOME%/jdk/bin 目录下执行该命令。

（2.2）回车后输入 PFX 证书密码，即密码文件 password.txt 中的内容。

说明 JKS 证书密码等同于 PFX 证书密码。两个密码不同的时候会导致 Tomcat 重启失败。

3、在 Tomcat 安装目录下新建 cert 目录，将转化后的证书文件和密码文件拷贝到 cert 目录下 。

4、修改配置文件 server.xml（路径：Tomcat 安装目录/conf/server.xml），并保存。

4.1、去掉以下内容的注释：

```
<Connector  port="8443"

protocol="HTTP/1.1"

 port="8443" SSLEnabled="true"

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

```
clientAuth="false" sslProtocol="TLS" /
```

4.2 参照以下内容修改<Connector port="443"标签内容：

```
<Connector port="443"  #port 属性根据实际情况修改（https 默认端口为 443）。如果使用其他端口号，则您需要使用 https://yourdomain:port 的方式来访问您的网站。

  protocol="HTTP/1.1"

  SSLEnabled="true"

  scheme="https"

  secure="true"

  keystoreFile="Tomcat 安装目录/cert/domain name.jks" #证书名称前需加上证书的绝对路径，请使用您证书的文件名替换 domain name。

  keystorePass="证书密码"  #此处请替换为您证书密码文件 pfx-password.txt 中的内容。

  clientAuth="false"

  SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"

  ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256"/>
```

5、可选： 配置 web.xml 文件，开启 HTTP 强制跳转 HTTPS。

在文件</welcome-file-list>后添加以下内容：

```
<login-config>

  <!-- Authorization setting for SSL -->

  <auth-method>CLIENT-CERT</auth-method>

  <realm-name>Client Cert Users-only Area</realm-name>  </login-config>  <security-constraint>

  <!-- Authorization setting for SSL -->

  <web-resource-collection >
```

```
    <web-resource-name >SSL</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>  </security-constraint>
```

6、重启 Tomcat。

执行以下命令关闭 Tomcat 服务器。

./shutdown.sh

执行以下命令开启 Tomcat 服务器。

./startup.sh

.