Tomcat 服务器安装 SSL 证书

环玺信息科技（上海）有限公司

GlobalSign China Co., Ltd

目 录

本文将全面介绍如何在 Tomcat 服务器配置 SSL 证书，具体包括在 Tomcat 上配置证书文件、证书密码等参数介绍，以及安装证书后结果的验证。成功配置 SSL 证书后，您将能够通过 HTTPS 加密通道安全访问 Tomcat 服务器。

重要：本文以 CentOS 7.9 64 位操作系统、Tomcat 9.0 为例介绍。不同版本的操作系统或 Web 服务器，部署操作可能有所差异。

前提条件

拥有证书，若您没有证书，请联系您购买证书时所对应的销售人员进行咨询。

- **证书文件（JKS 格式）**

步骤一：在 Tomcat 服务安装置证书

1. 上传证书文件到 Tomcat 服务器的 conf 目录
2. 进入 Tomcat 安装根目录，执行以下命令，打开 server.xml 文件

```
vim ./conf/server.xml
```

3. 在 server.xml 文件中，定位到以下配置项，按照配置示例进行配置

◆ 配置项一：

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443"
           maxParameterCount="1000"
           />
```

配置示例：

```
<Connector port="80" protocol="HTTP/1.1" #将 Connector port 修改为 80
               connectionTimeout="20000"
               redirectPort="443"  #将 redirectPort 修改为 SSL 默认端口
443，让 HTTPS 请求转发到 443 端口。
               maxParameterCount="1000"
               />
```

◆ 配置项二：

```
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
           maxThreads="150" SSLEnabled="true"
           maxParameterCount="1000"
           >
    <SSLHostConfig>
        <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"
                     type="RSA" />
    </SSLHostConfig>
</Connector>
-->
```

配置示例（需要去掉<!- - 和 - ->注释符）

```
<Connector port="443"
#将 Tomcat 中默认的 HTTPS 端口修改为 443。8443 端口不可通过域名直接访问、需要在域名后加上端口号。
#443 端口是 HTTPS 的默认端口，可通过域名直接访问，无需在域名后加端口号。
               protocol="org.apache.coyote.http11.Http11NioProtocol"
               #Connector port 有两种运行模式 NIO 和 APR，请选择 NIO 模式。
               maxThreads="150" SSLEnabled="true"
               maxParameterCount="1000"
               >
        <SSLHostConfig>
                              #修改为证书文件路径。
                <Certificate certificateKeystoreFile="conf/xxx.jks"
                              #填写证书文件密码。
                              certificateKeystorePassword="xxxxxx"
                              type="RSA" />
        </SSLHostConfig>
</Connector>
```

◆ 配置项三：

```
<!--
<Connector protocol="AJP/1.3"
           address="::1"
           port="8009"
           redirectPort="8443"
           maxParameterCount="1000"
           />
-->
```

配置示例（需要去掉<!- - 和 - ->注释符）

```
<Connector protocol="AJP/1.3"
               address="::1"
               port="8009"
               #将 redirectPort 修改为 443，让 HTTPS 请求转发到 443 端口。
               redirectPort="443"
               maxParameterCount="1000"
               />
```

4. 可选：在/conf/web.xml 文件，配置 HTTP 请求跳转 HTTPS

①. 进入到 tomcat 安装根目录下，执行以下命令，打开 web.xml 文件

```
vim ./conf/web.xml
```

②. 在 web.xml 文件<web-app>标签内添加以下配置项

```
<security-constraint>
         <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>
```

5.进入 Tomcat 的 bin 目录，执行以下命令，停止 Tomcat 并重启

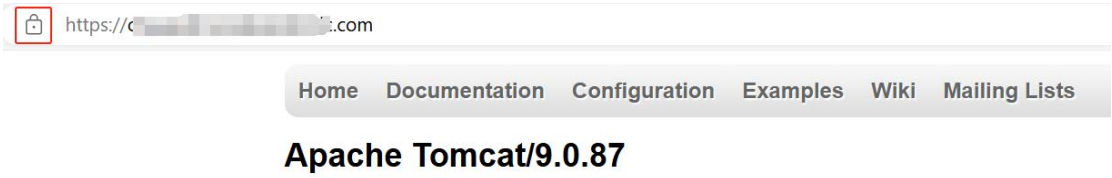
```
./shutdown.sh #停止 Tomcat 服务
./startup.sh #重启 Tomcat 服务
```

步骤二：验证 SSL 证书是否安装成功

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。

```
https://yourdomain    #需要将 yourdomain 替换成证书绑定的域名
```

如果网页地址栏出现小锁标志，表示证书已经安装成功。



技术支持邮箱地址:support-china@globalsign.com

文档支持站点地址:https://www.globalsign.cn/resources/installation