
Tomcat SSL 证书部署指南



沃通电子认证服务有限公司

WoSignCA Limited

目录

一、 安装 SSL 服务器证书.....	3
1.1 获取 SSI 证书.....	3
1.2 安装 SSL 证书环境.....	3
1.3 部署 SSL 证书.....	5
1.3.1 Tomcat 8.5 之前版本.....	5
1.3.2 Tomcat 8.5 及之后版本.....	6
二、 SSL 证书的备份.....	8
三、 SSL 证书的恢复.....	8

技术支持联系方式

技术支持邮箱：support@wosign.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 SSI 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，当中有包含五种证书

格式如：for Apache、for IIS、for Ngnix、for Tomcat、for Other Server；Tomcat 应用服务器上只需要 for Tomcat 里面的 JKS 证书文件即可。



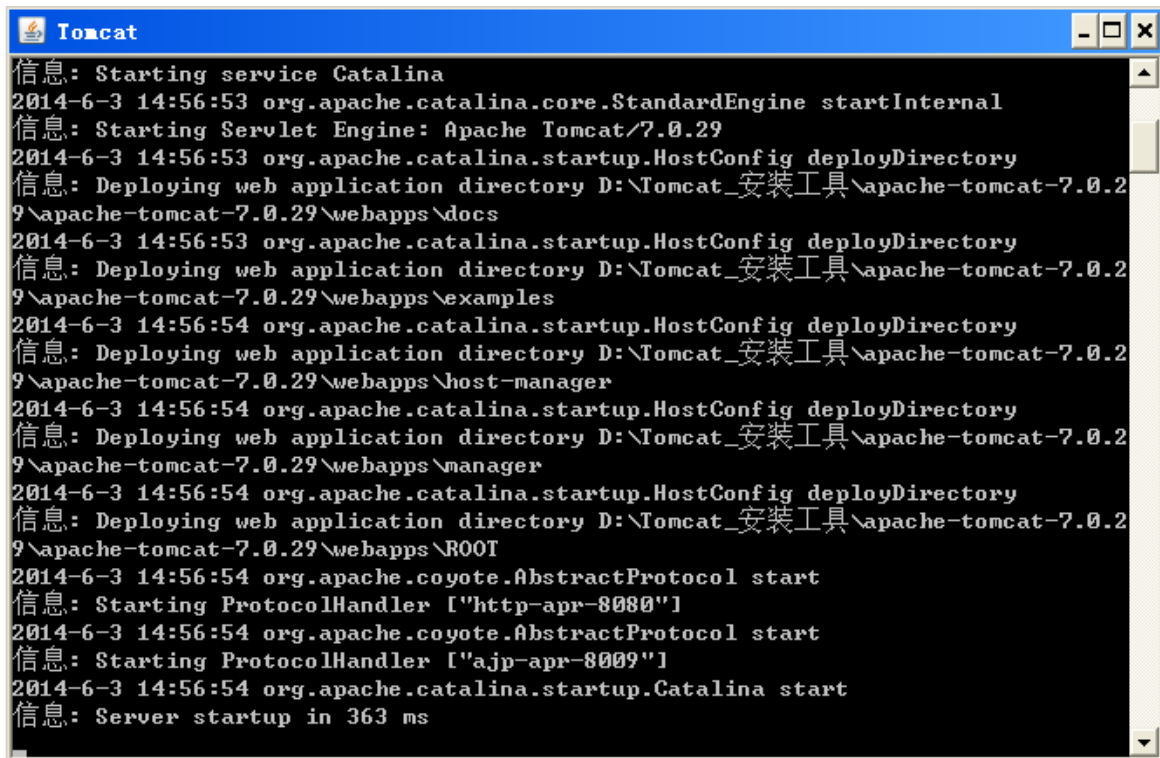
for Apache.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for IIS.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Ngnix.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Other Server.zip	2014/8/20 14:00	WinRAR ZIP 压缩...
for Tomcat.zip	2014/8/20 14:00	WinRAR ZIP 压缩...

图 1

1.2 安装 SSL 证书环境

首先访问 Tomcat 官网（<http://tomcat.apache.org/>）当前可根据您的系统下载不同的应用程序包，我们以 Windows 系统为例。所以下载 Windows 版本的 **apache-tomcat-7.0.29** 版本。

下载 Tomcat 解压到其中一个盘符下后，进入 apache-tomcat-7.0.29 根目录下找到 bin 文件中此执行文件 windows：“startup.bat”（linux：“startup.sh”），运行期间将出现如图 1 所示的命令提示符窗口。（由于 jdk1.6 不支持新型的加密算法，建议安装 Tomcat7.0+JDK1.7.0_45）。



```
Tomcat
信息: Starting service Catalina
2014-6-3 14:56:53 org.apache.catalina.core.StandardEngine startInternal
信息: Starting Servlet Engine: Apache Tomcat/7.0.29
2014-6-3 14:56:53 org.apache.catalina.startup.HostConfig deployDirectory
信息: Deploying web application directory D:\Tomcat_安装工具\apache-tomcat-7.0.29\apache-tomcat-7.0.29\webapps\docs
2014-6-3 14:56:53 org.apache.catalina.startup.HostConfig deployDirectory
信息: Deploying web application directory D:\Tomcat_安装工具\apache-tomcat-7.0.29\apache-tomcat-7.0.29\webapps\examples
2014-6-3 14:56:54 org.apache.catalina.startup.HostConfig deployDirectory
信息: Deploying web application directory D:\Tomcat_安装工具\apache-tomcat-7.0.29\apache-tomcat-7.0.29\webapps\host-manager
2014-6-3 14:56:54 org.apache.catalina.startup.HostConfig deployDirectory
信息: Deploying web application directory D:\Tomcat_安装工具\apache-tomcat-7.0.29\apache-tomcat-7.0.29\webapps\manager
2014-6-3 14:56:54 org.apache.catalina.startup.HostConfig deployDirectory
信息: Deploying web application directory D:\Tomcat_安装工具\apache-tomcat-7.0.29\apache-tomcat-7.0.29\webapps\ROOT
2014-6-3 14:56:54 org.apache.coyote.AbstractProtocol start
信息: Starting ProtocolHandler ["http-apr-8080"]
2014-6-3 14:56:54 org.apache.coyote.AbstractProtocol start
信息: Starting ProtocolHandler ["ajp-apr-8009"]
2014-6-3 14:56:54 org.apache.catalina.startup.Catalina start
信息: Server startup in 363 ms
```

图 1

启动执行文件后，我们将输入 Tomcat 应用服务默认的地址如：<http://127.0.0.1:8080>

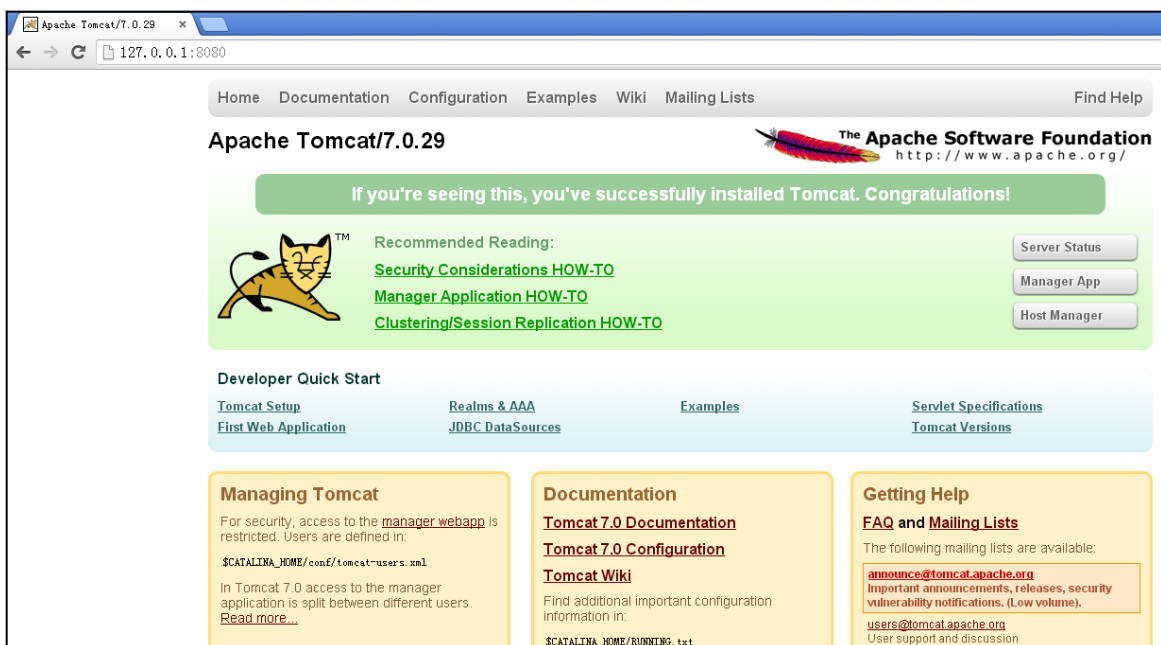


图 2

若有出现 Tomcat 默认此界面，则表示您当前的应用服务是正常可运行。

1.3 部署 SSL 证书

1.3.1 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:

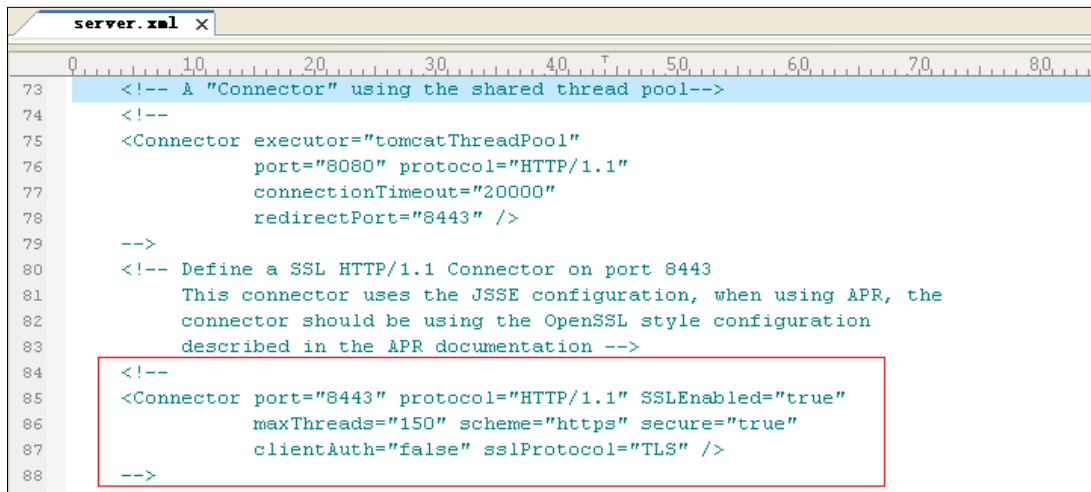


图 12

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

1.3.2 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，比如：

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="alias"
      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

- 加密协议和安全套件：<https://bbs.wosign.com/thread-1284-1-1.html>
- 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密码，以防丢失

三、 SSL 证书的恢复

重复第 1.3 步操作即可。