



Tomcat SSL 证书部署指南



WoTrus CA Limited

©2004-2017 沃通电子认证服务有限公司 WoTrus CA Limited All Rights Reserved

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



目录

<u> </u> ,	安装 SSL 服务器证书 3
	1.1 获取 SS1 证书 3
	1.2 部署 SSL 证书5
	1.2.1 Tomcat8.5 之前的版本5
	1.2.2 Tomcat8.5 及之后的版本 6
<u> </u>	SSL 证书的备份
Ξ,	SSL 证书的恢复

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。

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



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:

📑 for Apache.zip	2019/1/21 14:15	ZIP 文件	6 KB
📑 for Nginx.zip 🔶 解压此文件	2019/1/21 14:15	ZIP 文件	6 KB
afor Other Server.zip	2019/1/21 14:15	ZIP 文件	7 KB

图 1

打开 for Nginx 文件可以看到公钥,如图 2

test.wosign.com_bundle.crt	2017/11/27 15:27	安全证书	6 KB

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

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



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)

 ● 转换证 	時格式 〇 安装证书	○创建SPC/证书和	<u>1</u>	EUT:	文本框中粘贴证书内	睿(PEM 相式):	
原始格式: 目标格式:	PEM O DER O PEM O DER O	PFX JKS PFX ④ JKS (副名:1	7				
证书文件:	D:\for nginx\yourdoma	in.com_bundle.crt	选择				
私钥文件:	D:\for nginx\yourdoma	in.com.k e y	选择				
私胡密码:							
JKS密码:	*****]				
3.			-				

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。

File name:	yourdomain.com.jks		
Save as type:	JKS(*.jks)		
	-434	×	
e Folders		Save	Cancel

最后,得到 jks 格式证书。

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



🖉 ssl.key	2018/4/17 17:37	KEY 文件
test.wosign.com.jks	2018/4/17 17:38	JKS 文件
test.wosign.com_bundle.crt	2017/11/27 15:27	安全证书

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:

	server.xml ×
	Q
73	A "Connector" using the shared thread pool
74	</th
75	<connector <="" executor="tomcatThreadPool" th=""></connector>
76	port="8080" protocol="HTTP/1.1"
77	connectionTimeout="20000"
78	redirectPort="8443" />
79	>
80	Define a SSL HTTP/1.1 Connector on port 8443</th
81	This connector uses the JSSE configuration, when using APR, the
82	connector should be using the OpenSSL style configuration
83	described in the APR documentation>
84	</th
85	<connector <="" port="8443" protocol="HTTP/1.1" sslenabled="true" th=""></connector>
86	maxThreads="150" scheme="https" secure="true"
87	clientAuth="false" sslProtocol="TLS" />
88	>

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"

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



让互联网更加安全可信

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:

Apache Tomcat/7.0.29 ×					
← → C A https://decountertife.com					
Home Documentation	Configuration	Examples Wiki Mailing Lists			
Apache Tomcat/7	.0.29				
证书 常规 详细信息 证书路径	ı're seeing this	is, you've successfully installed Tomca			
证书信息 这个证书的目的如下: •保证远程计算机的身份	commended Rea curity Considerat nager Application Istering/Session	ading: <u>ttions HOW-TO</u> on HOW-TO I Replication HOW-TO			
* 有关详细信息,请参考证书颁发机构的说明。	<u>Realms & A</u> JDBC DataS	AAA <u>Examples</u> ISources			
微发者: WoSign Class 1 DV Server CA 有效起始日期 2014-5-30 到 2015-5-30		Documentation			
「 颁发者说明(S) 确定	anager webapp is n: •s. xml Ianager	<u>Tomcat 7.0 Documentation</u> <u>Tomcat 7.0 Configuration</u> <u>Tomcat Wiki</u>			

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

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



置 如图 14:

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

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



最后保存该配置文件,然后重启 Tomcat 后再次访问即可。如图 5

Apache Tomcat/7.0.29 ×					
← → C Attps://dumgumuk-111.htmm					
Home Documentation	Configuration	Examples Wiki Mailing Lists			
Apache Tomcat/7	.0.29	Th			
	I're seeing this	s, you've successfully installed Tomcat			
证书信息 这个证书的目的如下: •保证远程计算机的身份	commended Rea <u>curity Considerat</u> nager Application Istering/Session I	ding: ions HOW-TO h HOW-TO Replication HOW-TO			
* 有关详细信息,请参考证书颁发机构的说明。 優发给 : (14) 優发者 : WoSign Class 1 DV Server CA	<u>Realms & A</u> JDBC DataS	AA Examples Sources			
有效起始日期 2014-5-30 到 2015-5-30 颁发者说明(5)	a <u>nager webapp</u> is n:	Documentation Tomcat 7.0 Documentation Tomcat 7.0 Configuration			
	∙s.xml Nanager	Tomcat Wiki			

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: <u>https://bbs.wosign.com/thread-1284-1-1.html</u>

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。

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502