WAS服务器证书安装配置指南

服务器 SSL 证书安装配置指南

Websphere Application Server 7

更新日期: 2016-11-7

第一步: 生成证书请求文件(CSR)

进入 Java_JRE\bin 目录,如 cd C:\PROGRA~1\Java\jre1.5.0_06\bin,运行如下命令:

keytool -genkey -alias ssl -keyalg RSA -keysize 2048 -keystore c:\ssl.jks 输入 keystore密码: *******

您的名字与姓氏是什么? [Unknown]: cn.globalsign.com 您的组织单位名称是什么? [Unknown]: IT Dept. 您的组织名称是什么? [Unknown]: 您所在的城市或区域名称是什么?

[Unknown]: Shanghai 您所在的州或省份名称是什么?

[Unknown]: Shanghai

该单位的两字母国家代码是什么

[Unknown]: CN

您的名字与姓氏是什么?(这里输入域名,如: cn.globalsign.com) 您的组织单位名称是什么?(这里输入部门名称,如:IT Dept) 您的组织名称是什么?(这里输入公司名称名称,如: o., Ltd.) 您所在的城市或区域名称是什么?(这里输入城市,如: Shanghai) 您所在的州或省份名称是什么?(这里输入省份,如: Shanghai) 该单位的两字母国家代码是什么?(这里输入 2位国家代码,如: CN)

CN=cn.globalsign.com, OU=IT Dept, O= o., Ltd., L=Shanghai, ST=Shanghai, C=CN 正确吗?

[否]: Y

请核对信息,如果确认无误后请直接输入 Y并回车

输入< ssl >的主密码

(如果和 keystore密码相同,按回车):

不需要另外设置独立密码,这里回车即可,完成后在C盘根目录下就会生成一个 ssl.jks的 JAVA 证书池文件,在证书办法并导入前请妥善保存此文件。

keytool -certreq -alias ssl -keystore c:\ssl.jks -file c:\certreq.csr 输入 keystore密码: *******

输入密码后回车,这时会生成一个 certreq.csr的文件,此文件为证书请求文件(CSR)。

第二步: 提交 CSR, 申请证书

递交证书申请表及相关资料,并把证书请求文件(CSR)提交给我们。 我们确认资料齐全后,三个工作日内完成证书颁发。

第三步:获取服务器证书

1. 获取中级证书(此证书由GlobalSign系统通过Email方式发送给用户,邮件中第二段代码),证 书文件的内容为(包括"-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----"),请把此内 容保存为 intermediate.cer(文本格式)。

keytool -import -trustcacerts -keystore c:\ssl.jks -alias inter -file intermediate.cer

2. 获取SSL证书(此证书由GlobalSign系统通过Email方式发送给用户,邮件中第一段代码),证书 文件的内容为(包括"-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----"),请把此内容 保存为 server.cer(文本格式)。

keytool -import -trustcacerts -keystore c:\ssl.jks -alias ssl -file server.cer

第三步全部完成后,表示证书已经完全安装到 ssl.jks这个文件中,请备份此文件并妥善保存, 以后如有更换服务器或重装系统,就可以直接使用此文件。

第四步:安装服务器证书

将合成好的 JKS文件导入到服务器上

打开"管理控制台",输入管理帐户,点击"登录",

🚰 集成解	决方案控制	【台 - ∎i	crosoft I	nternet l	xplorer
文件 (E)	编辑(E)	查看 (V)	收藏(A)	工具(T)	帮助(出)
③ 后退 、	- 🕤 - 💌	1 🗈 🐔	🔎 搜索	☆ 收藏夹	· 😔 🛛 😥 •
地址 (2)	🛐 https:/	/localhost	t:9043/ibm,	console/lo	gon. jsp
Integrated	I Solutions	Console			
欢迎使 用户标证	用,请 输 _{兄:}	前入您的	信息。 —		
│ 密码: │			_		
登录					

在"安全性"下,点击"SSL证书和密钥管理"



点击"管理端点安全配置"

SSL 配置
安全套接字层(SSL)协议在远程服务器进程或端点。 建立安全通信,必须对该端点指定证书和 SSL 配置。
在本产品的先前版本中,需要为每个端点手动配置安约 置。此功能使您能够集中管理安全通信。另外,通过?
如果已使用迁移实用程序将受保护的环境迁移到此版2 配置 SSL 才能利用集中管理功能。
配置设置
管理端点安全配置
管理证书到期
□ 使用美国联邦信息处理标准(FIPS)算法。注意;
☑ 当发生 SSL 配置更改时动态更新运行时
应用 复位

在"本地拓扑"下的"入站"下,选择"Server1"

SSL 证书和密钥管理 > 管理端点安全配置

显示所选作用域的安全套接字层 (SSL) 配置, 例如, 单



在屏幕右侧点击"密钥库和证书"



点击"NodeDefaultKeyStore"

SSL 证书和密钥管理	
<u>SSL 证书和密钥管理</u> > <mark>管理端点竖</mark> 定义密钥库类型,包含密码术、RACF	<mark>2全配置</mark> > <u>ser</u> (R)、CMS、Jav
密钥库的用法	
CCI 恋妇房 ,	
SSL 密钥库	
田 首诜项	
新建 删除 更改密码	交换签署者
选择 名称 ≎	描述 ≎
您可以管理以下资源:	
NodeDefaultKeyStore	fastcom-was 密钥库
□ <u>NodeDefaultTrustStore</u>	fastcom-was 信任库
3.4.34	1

在页面右边的"其他属性"中点击"个人证书"

· <u>签署者证</u>书

- 个人证书请求

• 个人证书

■ 定制属性

其他属性

_

点击"导入"

21	速 -	凱除	从认证中	心发妆	著换 3	触取 ()	.	±
选择			划名	须发给		发放者	\smile	序列
愈同	[以管理	以下资源						
C			defaut	CN=192, OU=Fest wasNode OU=Fest wasNode C=US	168,133,125, com- 01Cell, com- 01, 0=IBM,	CN=192 DU=Reci OU=fasti wasNode C=US	168,133,129, t Certificate, tom- 01Cell, tom- 01, D=IBM,	163
	না			CN=192. OU=Roo OU=fast ovasNode OU=fast ovasNode	168.133.125, L Certificate, com- 01Cell, com- C1, Ω=IBM,	CN=192. DU=Rcc OU=fasti vasNode OU=fasti vasNode	168.133.129, I Certificate, tom- 01Cell, tom- 01, D=1844,	163

页面帮助

关于此页面的更多

输入 JKS文件的位置: "c:\ssl.jks",类型选择"JKS",输入保护密码,然后点击"获取密钥文件别名"

C 受會密钥库 密钥库	
NodeDefaultKeyStore ((cel 密钥库图码	l):fastcom-wasNode01Cell:(no
 密钥庫文件 密钥库文件 · 密钥文件名 (c:\ssl.jks) 大型 JKS 密钥文件密码 	
 ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	(获取密钥立件别名

WAS会从 JKS文件中读取密钥对的别名,选择 JKS中的密钥对别名,并输入导入到 WAS后的别名,然 后点击"确定"

C 受管密销库 密销库	
NodeDefaultKeyStore ((cell):f	astcom-wasNode01Cell:(nod
密组库密码	
- Mundar Apple Status Andreas	
6 密铜库文件	
+ 密钥文件名	
c:\ssl.jks	
类型 (二)	
JKS 🔹	
+ 密钥文件密码	
••••	获取密钥文件别名
ELAMIE BALL	
sel T	
导人的证书别名	

这时可以看到,WAS中多了一个 SSL别名的密钥对,点击"保存"到主配置

onsole	admin, 欢迎您
n-was	NodeO1Cell,概要文件 = AppSrvO1
锂	
日消息	₫
	⚠️已更改了您的本地配置。您可以: 直接
(• 保存到主配置。
	 查看更改。
	⚠️要使这些更改生效,可能需要重新启动服务器。

<u> 密钥管理</u> > 管理端点安全配置 > <u>server1</u> > 密钥库和

选中"default"别名,点击"替换"

SSL 证书和密钥管理

SSL证书和密制 管理个人证书。 田首选项 创建・	<u>]管理</u> > 1 除 り	管理端点安全配置 > server1 > 密钥
选择	别名	颁发给
您可以管理以下	资源:	
	<u>default</u>	CN=192.168.133.129, OU=fastcom-wasNode01Cell, OU=fastcom-wasNode01, O=IBM, C=US
î		CN=192.168.133.129, OU=Root Certificate, OU=fastcom- wasNode01Cell, OU=fastcom- wasNode01, O=IBM, C=US

选择"替换为'SSL'",点击"确定"



点击"保存"到主配置

m-wasNo 管理 口消息	deO1Cell, 概要文件 = AppSrvO1
管理 回消息	
日消息	
山口	更改了您的本地配置。您可以:
	保存到主配置。
保在	<u>字或放弃之前</u> 本差要改
• 1	<u>自有</u> 史风。 要使这些更改生效,可能需要重新启动服务器。

<u> 密钥管理</u> > 管理端点安全配置 > <u>server1</u> > 密钥库和

重新启动 WAS服务器进程,证书已经替换上去了

按照以上的步骤配置完成后就可以使用https://www.domain.com来访问了。 如有任何问题或疑问请直接与我们联系,谢谢!