

Weblogic 10

二〇二一年一月



目录

| 1. 生成证书请求 | |
|-------------------|----|
| 1.1 安装JDK(可选) | |
| 1.2 生成keystore 文件 | |
| 1.3 生成证书请求文件(CSR) | |
| 2. 导入服务器证书 | 4 |
| 2.1 获取中级CA 证书 | 4 |
| 2.2 获取服务器证书 | 4 |
| 2.3 导入证书 | 5 |
| 3. 安装服务器证书 | 6 |
| 3.1 配置Servers | 6 |
| 3.2 设置认证模式 | |
| 3.3 设置服务器证书私钥别名 | 10 |
| 3.4 访问测试 | 11 |
| 4. 服务器证书的备份及恢复 | 11 |
| 4.1 服务器证书的备份 | |
| 4.2 服务器证书的恢复 | |



服务器证书安装配置指南(Weblogic 10)

1. 生成证书请求

1.1 安装JDK (可选)

Weblogic 安装后自带JDK 安装。如果您直接在服务器上生成证书请求,请进入Weblogic安装目录

下JDK 所在路径的bin 目录,运行keytool 命令。

如果您需要在其他环境下生成证书请求文件,则您可以选择安装JDK,并稍后上传生成的密钥库文件

keystore.jks 到服务器上进行配置。

可以参考Java SE Development Kit (JDK) 下载。下载地址:

http://java.sun.com/javase/downloads/index.jsp

1.2 生成keystore 文件

生成密钥库文件keystore.jks 需要使用JDK 的keytool 工具。命令行进入JDK 下的bin目录,运行

keytool 命令。(示例中粗体部分为可自定义部分,请根据实际配置情况作相应调整)

keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore keystore.jks -storepass

password

| keytoo -genke 输入 keystore { | y -alias weblogickeyalg RSAkeysize 2048 -keystore c:\ca\keystore.jks 密码: ****** |
|---------------------------------|--|
| | |
| 您的名字与姓日 | 5是什么? |
| [Unknown]: | cn.globalsign.com |
| 您的组织单位名 | 3称是什么? |
| [Unknown]: | IT Dept. |
| 您的组织名称是 | 晶什么? |
| [Unknown]: | GlobalSign China Co., Ltd. |
| 您所在的城市或 | 载区域名称是什么? |
| [Unknown]: | Shanghai |
| 您所在的州或省 | 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 |



| CN=cn.globalsign.com, OU=IT Dept, O= GlobalSign China Co., Ltd., L=Shanghai, ST=Shanghai, C=CN 正确吗? [否]: Y |
|--|
| 输入 <weblogic>的主密码 (如果和 keystore 密码相同,按回车):</weblogic> |

以上命令中, server 为私钥别名(alias), 生成的keystore.jks 文件默认放在命令行当前路径下。

1.3 生成证书请求文件(CSR)

keytool -certreq -alias server -sigalg MD5withRSA -file certreq.csr -keystore keystore.jks -

keypass password -storepass password



请将证书请求文件certreq.csr 提交给GlobalSign , 并备份保存证书密钥库文件keystore.jks , 等待证

书的签发。密钥库文件丢失将导致证书不可用。

2. 导入服务器证书

2.1 获取中级CA 证书

为保障服务器证书在 IE7 以下客户端的兼容性,服务器证书需要安装两张中级 CA 证书(包括中级 证书和交叉证书)。

从邮件中获取中级证书和交叉证书:

将证书签发邮件中的从 BEGIN 到 END 结束的两张中级 CA 证书内容 (包括"-----BEGIN

CERTIFICATE-----"和"-----END CERTIFICATE-----")分别粘贴到记事本等文本编辑器中,并修改文



件扩展名,保存为 intermediate1.cer (交叉证书)和 intermediate2.cer (中级证书)文件。

2.2 获取服务器证书

将证书签发邮件中的从 BEGIN 到 END 结束的服务器证书内容 (包括"-----BEGIN CERTIFICATE--

--"和"-----END ERTIFICATE-----")粘贴到记事本等文本编辑器中,并修改文件扩展名保存为

server.cer文件。

查看Keystore文件内容

进入 JDK 安装目录下的 bin 目录,运行 keytool 命令。

您的keystore 密码

keytool -list -keystore C:\keystore.jks -storepass password



查询到 PrivateKeyEntry 属性的私钥别名(alias)为server。记住该别名,在稍后导入服务器证书时需

要用到。(示例中粗体部分为可自定义部分,请根据实际配置情况作相应调整。)

注意,导入证书时,一定要使用生成证书请求文件时生成的 keystore.jks 文件。keystore.jks 文件 丢失或生成新的 keystore.jks 文件,都将无法正确导入您的服务器证书。

2.3 导入证书

导入第一张中级 CA 证书 (交叉证书)

keytool -import -alias intermediate1 -keystore C:\keystore.jks -trustcacerts -storepass



password -file C:\intermediate1.cer

导入第二张中级 CA 证书(中级证书)

keytool -import -alias intermediate2 -keystore C:\keystore.jks -trustcacerts -storepass

password -file C:\intermediate2.cer



导入服务器证书

私钥的别名

keytool -import -alias server -keystore C:\keystore.jks -trustcacerts -storepass

password -file C:\server.cer



导入服务器证书时,服务器证书的别名必须和私钥别名一致。请留意导入中级CA 证书和导入服务器 证书时的提示信息,如果您在导入服务器证书时使用的别名与私钥别名不一致,将提示"认证已添加至 keystore 中"而不是应有的"认证回复已安装在keystore 中"。证书导入完成,运行keystool 命令,



再次查看keystore 文件内容

keytool -list -keystore C:\keystore.jks -storepass password



3. 安装服务器证书

3.1 配置Servers

登陆Weblogic 控制台,并进入 "Servers"





选择您需要配置服务器证书的Server

| 💫 👻 🙋 http://192.166.16.1:7001/c | onsole/conso | le.portal?_nfpb=tr | ue@_pageLa | bel=CoreSe | verServerTa | blePage | ¥ 4 |
|--|----------------------|--|------------|-----------------------------------|-------------------------------|------------|----------------|
| 🛠 🔏 Sunnary of Servers - vl_serve | r - WLS Cons | ole | ł | a • 📾 | - 🖶 - 🖂 | 页面 (2) | • 🎯 IR Q |
| M_server B-Environments H-Services Security Realms B-Interoperability B-Diagnostics | Mach This Webi | nine (JVM) and has it page summarizes e Logic Server domain comize this table rs (Filtered - More (W Clane D | Columns Ex | iguration. that has be ist) | en configure wing 1 to 1 o | d in the c | ument |
| | | Name 🌣 | Cluster | Machine | State | Health | Listen Port |
|) | | examplesServer (admin) | | | RUNNING | 🗖 ок | 7001 |
| How do I 💌 | Ne | W Clone D | elete | Sho | wing 1 to 1 o | f1 Previ | ous Next |
| Create Managed Servers | | | | | | | |
| Delete Managed Servers | | | | | | | |
| Delete the Administration Server | | | | | | | |

在 "General" 下,可以配置您的http 和https 是否启用,以及访问端口号。https 默认端口号为443,

请在选项启用SSL 并相应修改端口号。



| 오큐(@) Sniff(@) 오줌(@) 역(da,A(@) - (@) http://162.168.18.1:7001, | 上兵 (() 市助)(() /consola/console.portal?_mfpb=truck_pageLabel= | SerwerConfigGener al TabFage&handl e 💌 🐓 🔀 |
|---|---|---|
| 🍃 🖸 🏀 Settings for examplesServer | - vl_server | - 🖾 - 🖶 - 🕞 एक 😰 - 🎯 - 🖾 - |
| Failed (0) Critical (0) Overloaded (0) | Listen Port Enabled | Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. Nore Info |
| 0K (1) | Listen Port: 7001 | The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info |
| | SSL Listen Port Enabled | Indicates whether the server can be reached through the default SSL listen port. More Info |
| | SSL Listen Port: 7002 | The TCP/IP port at which this server listens for SSL connection requests. More into |
| | 🔲 🛃 Client Cert Proxy Enabled | Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info |
| | lava Compiler | |

3.2 设置认证模式

选择"Keystores",并配置认证方式。





服务器单向认证选择"Custom identity and Java Standard Trust", 双向认证请选择

"Custom Identity and Custom Trust" 。

将您的密钥库文件keystore.jks 保存到服务器上相应目录,并配置其路径和密钥库文件保护密码。

| 🕑 👻 🙋 http://152.168.18.1:7001/c | onsole/console.por | tal?_nfpb=truck_pageLabel=ServerConfigTabkeys | toreIabPageähe 🌱 🧌 |
|-----------------------------------|--------------------|--|---|
| 👙 🌈 Settings for examplesServer - | vl_server | 🙆 • 📾 • 🖨 • 🔂 | 页面的 - 💮 1具の |
|) | Keystores: | Custom Identity and Java Standard Trust | Which configurat |
| How do I 🖪 | | Custom Identity and Command Line Trust Custom Identity and Custom Trust | used for finding t server's identity a |
| Configure identity and trust | | Demo Identity and Demo Trust | More Info |
| Set up SSL | - Identity | | |
| | Custom Identity | C:\keystore.jks | The path and file name of the iden |
| Current Carrier | Reystore. | | Into |
| System Status | Custom | | The type of the |
| Health of Running Servers | Identity | jks | keystore. Genera |
| Falled (0) | Type: | | Info |
| Overloaded (0) | Custom | | The encrypted |
| Warning (0) | Keystore | | custom identity keystore's |
| 0K (1) | Passphrase: | | passphrase. If empty or null, the |
|) | | | opened without a |

单向认证中,需要配置JRE 默认信任库文件cacerts。Cacerts 默认密码为changeit。



| • E http://122.168.18.1:7001/conzole/conz | le.portal?_nfpb=truck_pageLabel=ServerConfig | labkeystorelabPageahe 💙 🐓 |
|---|---|---|
| Java Stand Trust Keyst | C:\beaUROCKI~1\jreVib\security\cacerts ard pre: | The path and file name of the trust keystore. More Info |
| Java Stand Trust Keyst Type: | Jks ore 默认密码 | The type of the keystore. Genere this is KS. Moi : changeit |
| Java Stand Trust Koyst Pass | ard ••••••• | The password fo the Java Standar Trust keystore. T password is defined when the keystore is created. More info |
| Confi Java Stand Trust Keyst Pasia | mard | |

3.3 设置服务器证书私钥别名

在 "SSL" 下需要配置密钥库中的私钥别名信息。私钥别名可以使用keystool -list 命令查看。通常设

置的私钥保护密码和keystore 文件保护密码相同。



| 💽 🗸 👩 http://122.168.18.1:7001/- | console/console.port | al? nfpb=truck pageLab | el=ServerConfigTabSSLT | abFageåhandle= 👻 🍫 |
|---|---|--|---|------------------------|
| 🐇 🌈 Settings for examplesServer - | vl_server | 1 | • • • • • | 反面(2) ・ ② ゴ具(2) |
| Future changes will automatically be activated as you modify, add or delete items in this domain. | Settings for | examplesServer | | |
| | Configuration | Protocols Logging | Debug Monitoring | Control |
| Domain Structure | Deployments | Services Security | Notes | |
| wl_server | General Clu | ster Services Keys | tores SSL Federatio | n Services |
| B-Environment Deployments | Deployment | Migration Tuning (| Verload Health Monito | ring |
| Services Security Realms | Server Start | | | |
| B-Interoperability B-Diagnostics | Save | | | |
| | This page le settings for t security of m | ts you view and define va his server instance. The essage transmissions. | rious Secure Sockets La se settings help you to ma | yer (SSL) anage the |
|] | Identity and | Keystores | | Indicates where |
| | Locations: | | | the server's |

设置私钥别名"server",并输入私钥保护密码。



| E Settings for examplesServer - | vl_server | 🖸 - 🖶 • 🕞 页面 🛛 • 💮 工具 🖸 |
|--|---------------------------------|--|
| System Status | | file. More info |
| Health of Running Servers Failed (0) Critical (0) Overloaded (0) Warning (0) OK (1) | Private Key Alias: | The keystore attribute that defines the string alias used to store and retrieve the server's private key. More Info The keystore attribute that defines the passphrase used to retrieve the server's rivate |
| | Confirm Private Key Passobrase: | key. More Info |

3.4 访问测试

在每一步设置过程中请注意随时保存所做的修改,完成所有配置后,就可以立即通过您设定的SSL端口号,访问https://youdomain:port测试证书的安装情况了。

4. 服务器证书的备份及恢复

在您成功的安装和配置了服务器证书之后,请务必依据下面的操作流程,备份好您的服务器证书,以

防证书丢失给您带来不便。

4.1 服务器证书的备份

备份服务器证书密钥库文件keystore.jks 文件即可完成服务器证书的备份操作。

4.2 服务器证书的恢复

请参照服务器证书安装部分,将服务器证书密钥库 keystore.jks 文件恢复到您的服务器



上,并修改配置,恢复服务器证书的应用。

请注意,此文档会不定期更新!

GlobalSign China Co., Ltd

环玺信息科技 (上海)有限公司

2021年1月