

数安时代科技股份有限公司

GDCA 信鉴易® SSL 服务器证书部署指南 For Weblogic 12版本

2015/11/23



目录

<i>—`</i> ,	部署前特别说明	2
<u> </u>	使用 KEYTOOL 工具产生证书请求	2
	1. 初始环境准备	2
	2. 产生密钥库文件	2
	3. 产生证书请求文件	4
三,	服务器证书的导入	5
	1. 获取服务器证书的根证书和 CA 证书	5
	1.1 从邮件中获取	5
	1.2从GDCA 官网上下载:	6
	1.3 转换证书编码	8
	2. 查看密钥库文件信息	11
	3. 导入证书	12
	4. 产生 truststore 文件(可选):	14
四、	安装服务器证书	15
	1. 单向 SSL	15
	1.1 配置服务器	15
	1.2 配置认证模式	17
	1.3 配置服务器证书私钥别名	19
	1.4 https 访问测试	19
	2. 双向 SSL	20
	2.1 配置服务器	20
	2.2 配置认证模式	21
	2.3 配置服务器证书私钥别名	22
	2.4 https访问测试	23
五、	备份和恢复	23
	1. 备份服务器证书	24
	2. 恢复服务器证书	24
$\frac{1}{1}$	证书遗失处理	

一、部署前特别说明

 GDCA 信鉴易[®] SSL 服务器证书部署指南(以下简称"本部署指南")主要描述 如何通过 openssl 产生密钥对和如何将 SSL 服务器证书部署到 weblogic 服务器
 本部署指南适用于 weblogic 12 版本;

 weblogic 服务器部署恒信企业 EV SSL 和睿信 SSL 证书的操作步骤一致,区 别在于:前者在 IE7 以上浏览器访问时,浏览器会显示安全锁标志,地址栏会变 成绿色;而后者在浏览器访问时,浏览器显示安全锁标志,但地址栏不会变成绿 色;

4. 本部署指南使用 testweb.gdca.com.cn 作为样例进行安装配置,实际部署过程请用户根据正式的域名进行配置;

5. 您可以使用其它方式并不要求按照本部署指南在 windows 下使用 Keytool 工 具产生密钥库文件以及生成证书请求文件。

6. 如用户已经生成证书请求文件,请从第三点服务器证书的导入开始阅读。

二、使用 KEYTOOL 工具产生证书请求

1. 初始环境准备

制作证书请求文件的工作环境,需要先安装好 JDK(请使用 1.6 或以上版本), 再使用 JDK 所在路径的 bin 目录下的 keytool 命令。

2. 产生密钥库文件

打开 windows 命令行窗口,进入 JDK 的 bin 目录运行 keytool 命令参考:

keytool -genkey -alias yourserver -keyalg RSA -keysize 2048 -keystore yourkeystore.jks -storepass yourpassword

-storepass 指定 keystore 密码

系统会提示您输入你的信息。填写信息说明:

1您的姓名与姓氏是什么?



填: 域名(公网访问的域名地址如 testweb.gdca.com.cn; 如果有多个域名, 只填主域名)

2您的组织单位名称是什么?

填:组织单位名或部门名(如技术支持部或 Technical Support)

3您的组织名称是什么?

填:组织名或公司名(数安时代科技股份有限公司或 Global Digital Cybersecurity Authority Co.,Ltd.)

4您所在的城市或者区域名称是什么?

填:城市或区域名(如佛山市或 Foshan)

5您所在的州或省份名称是什么?

填:州名或省份名(如广东省或 Guangdong)

6该单位的两字母国家代码是什么?

填:两位国家代码(如中国为CN,美国为US)

除第1、6项外,2-5的信息填写请统一使用中文或者英文填写,并确保内 容和您提交到 GDCA 的内容一致,以保证 SSL 证书的签发。

例:

keytool -genkey -alias testweb -keyalg RSA -keysize 2048 -keystore D:\keystore.jks -storepass 123456







示例中使用 testweb 作为私钥别名 (alias), 生成的密钥库文件名为 keystore.jks,该文件存放 D 盘下。注意:如果不指定目标路径, keystore.jks 会存放在命令行的当前路径下(这里是 keytool 所在目录)。

3. 产生证书请求文件

参考:

keytool -certreq -alias yourserver -keystore keystore.jks -file yourserver.csr -keypass yourpassword -storepass yourpassword

例:

keytool -certreq -alias testweb -keystore D:\keystore.jks -file D:\testweb.csr -keypass 123456 -storepass 123456

画 管理员: C:\Windows\system32\cmd.exe	
c:\Java\jdk1.6.0_45\bin>keytool -certreq -alias testweb -keysto s -file D:\testweb.csr -keypass 123456 -storepass 123456	re D:\keystore.jk
c:\Java\jdk1.6.0_45\bin>	

产生请求文件 testweb.csr

三、服务器证书的导入

1. 获取服务器证书的根证书和 CA 证书

服务器证书需要安装根证书和 CA 证书,以确保证书在浏览器中的兼容性。有两种方式获取。

1.1 从邮件中获取

在您完成申请 GDCA 服务器证书的流程后, GDCA 将会在返回给您的邮件中附 上证书的公钥以及根证书 GDCA_TrustAUTH_R5_ROOT. cer 和相应的 CA 证书。如果 您申请的是睿信(OV SSL)证书(Organization Validation SSL Certificate), CA 证书就是文件就是 GDCA_TrustAUTH_R4_OV_SSL_CA. cer; 如果您申请的是恒信 企业 EV SSL 证书(Extended Validation SSL Certificate), CA 证书就是文件 就是 GDCA_TrustAUTH_R4_EV_SSL_CA. cer, 请确认所收到的证书文件是您需要的 CA 证书。(注意:所发至邮箱的文件是压缩文件,里面有3张证书,请确认所收 到的证书文件是您需要的 CA 证书文件)

文件(E) 命令(C) 工具(S) 收藏夹(Q) 选项(N) 帮助	助(<u>H</u>)				
	=170	IN THE COLOR	22 1-1-1007500		#111034
🗳 📲 www.huizhou.gov.cn(1).rar\www.huizho	u.gov.cn	- RAR 压缩文	件, 解包大小为 6,	188 字节	
名称	大小	压缩后大小	类型	修改时间	CRC32
🎍 <u>.</u>			文件夹		
IGDCA TrustAUTH R4 EV SSL_CA.cer 中级证书	2,090	1,576	安全证书	2016/10/18 1	58479850
GDCA TrustAUTH R5 ROOT.cer	2,012	1,488	安全证书	2016/10/18 1	F8476090
IIII www.huizhou.gov.cn.cer 化证书 用户证书	2,086	1,473	安全证书	2016/10/18 1	FBCD26



GDCA_TrustAUTH_R4_OV_SSL_CA.cer:

吊規	详细信息	证书路径	
证书	路径(P)—		
-	GDCA Trust	AUTH RS ROOT	
	GDCA TI	rustAUTH R4 OV SSL CA	

GDCA_TrustAUTH_R4_EV_SSL_CA.cer:

常规	详细信息	证书路径	
ரு‡	· 路径(P)	0 0 -	
	GDCA TH	ustAUTH R4 EV SSL CA	
1			

1.2 从 GDCA 官网上下载:

 $\tt https://www.trustauth.cn/support/ca_cq/$

☆ 首页 / 技术支持 / C	A证书查询			
CA名称	起始有效时间	截止有效时间	CA证书下载	部署指南
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer	常见问题
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_SSL_CA.cer	常用工具
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_OV_SSL_CA.cer	CA证书查询
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_CodeSigning_CA.cer	
GDCA TrustAUTH R4 CodeSigning CA	2016-04-07 17:50:05	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA cer	
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer	

37项,显示1到10.[首页/前一页] **1**, <u>2</u>, <u>3</u>, <u>4</u> [下一页/末页]



获取根证书: GDCA_TrustAUTH_R5_ROOT.cer:

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_SSL_CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_OV_SSL_CA.cer
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_CodeSigning_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2016-04-07 17:50:05	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer

获取 CA 证书:

如果您申请的证书是睿信(OV) SSL证书(Organization Validation SSL Certificate),下载GDCA_TrustAUTH_R4_OV_SSL_CA.cer

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_SSL_CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_OV_SSL_CA.cer
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_CodeSigning_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2016-04-07 17:50:05	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer

为保证您的证书能够正常使用,需要为浏览器下载并安装CA根证书,这样你的浏览器才能信任由GDCA签发的所有证书(下载后双 击证书文件进行安装)。 37项,显示1到10.[首页/前一页] 1,2,3,4 [下一页/末页]

如果您申请的证书是恒信企业 EV SSL 证书 (Extended Validation SSL Certificate),则下载 GDCA_TrustAUTH_R4_EV_SSL_CA.cer





CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_SSL_CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_OV_SSL_CA.cer
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_EV_CodeSigning_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2016-04-07 17:50:05	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer

为保证您的证书能够正常使用,需要为浏览器下载并安装CA根证书,这样你的浏览器才能信任由GDCA签发的所有证书(下载后双 击证书文件进行安装)。

37 项,显示1到10.[首页/前一页] 1, 2, 3, 4 [下一页/末页]

1.3 转换证书编码

从官网上下载的证书需要先转换为 Base64 编码格式。以根证书为例: 打开证书:

*	▲ 证书信息			
×	 化证为时目时如下: 保证远程计算机的身 向远程计算机证明愈 确保软件来自软件发 保护软件在发行后不 	份 的身份 布者 被更改		*
<u> </u>	颁发给 : GDCA Tru 颁发者 : GDCA Tru	stauth R5 Root		;
	有效期从 2014/	11/ 26 到	2040/ 12/	31
		安装证书(I)	① 颁发者说	í明(S)

详细信息-复制到文件





■版本	V3 73 00 07 6, 60 47 7.
□ 序列号 警 签名算法 ■ 签名哈希算法	sha256RSA
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	GDCA TrustAUTH R5 ROOT, 2014年11月26日 13:13:15
	2040年12月31日 23:59:59

在证书导出向导里,将证书编码改成 Base64 编码格式







选择要	使用的格式:			
O	DER 编码二进制 X.509(.	CER) (<u>D</u>)		
۲	Base64 编码 X.509(.CER) <u>(c)</u>]		
6	加密消息语法标准 - PKC	S #7 证书(. P7B)(C)	
	🗌 如果可能,则数据包括	证书路径中的所有	证书(L)	
	个人信息交换 - PKCS #1	2 (. PFX) (<u>P</u>)		
	🗌 如果可能,则数据包括	证书路径中的所有	证书创	
	🗌 如果导出成功,删除利	4钥(K)		
	□ 导出所有扩展属性 (A)			
0	Microsoft 序列化证书存	储者(SST)(T)		

导出到指定目录里

证书导出向导	×
要导出的文件 指定要导出的文件名。	
文件名位): D:\GDCA_TrustAUTH_R5_ROOT.cer	[浏览 @)]

转换成 Base64 编码格式后,用编辑器打开,可以看到文件内容是以-----BEGIN CERTIFICATE----开头,----END CERTIFICATE----结尾。以同样方式将 CA 证书也转换成 Base64 编码格式。



---BEGIN CERTIFICATE--MIIFiDCCA3CgAwIBAgIIfQmX/vBH6nowDQYJKoZIhvcNAQELBQAwYjELMAkGA1UE BhMCQ04xMjAwBgNVBAoMKUdVQU5HIERPTkcgQ0VSVE1GSUNBVEUgQVVUSE9SSVRZ IENPLixMVEQuMR8wHQYDVQQDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMB4XDTE0 MTEyNjA1MTMxNVoXDTQwMTIzMTE1NTk10VowYjELMAkGA1UEBhMCQ04xMjAwBgNV ${\tt BAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZIENPLixMVEQuMR8w}$ ${\tt HQYDVQQDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMIICIjANBgkqhkiG9w0BAQEF}$ AAOCAg8AMIICCgKCAgEA2aMW8Mh0dHeb7zMNOwZ+Vfy1YI92hhJCfVZmPoiC7XJj Dp6L3TQsAlFRwxn9WVSEyfFrs0yw6ehGXTjGoqcuEVe6ghWinI9tsJlKCvLriXBj TnnEt1u9ol2x8kECK62pOqPseQrsXzrj/e+APK00mxqriCZ7VqKChh/rNYmDf1+u KU49tm7srsHwJ5uu4/Ts765/94Y9cnrrpftZTqfrlYwiOXnhLQiPzLyRuEH3FMEj $\verb+qcOtmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{eq:cotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{eq:cotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{eq:cotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{eq:cotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{eq:cotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{eq:cotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{eq:cotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{CotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{CotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{CotmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpmdesfactore{Constraint} \label{CotmkVEs7L} \label{CotmkVEs7$ MUHfP/vFBu8btn4aRjb3ZGM74zkYI+dndRTVdVeSN72+ahsmUPI2JgaQxXABZG12 ZuGR224HwGGALrIuL4xwp9E7PLOR5G62xDtw8mySlwnNR30YwPO7ng/Wi64HtloP zgsMR6flPri9fcebNaBhlzpBdRfMK5Z3KpIhHtmVdiBnaM8Nvd/WHwlqmuLMc3Gk L30SgLdTMEZeS1SZD2fJpcjyIMGC7J0R38IC+xo70e0gmu91ZJIQDSri3nDxGGeC jGHeuLzRL5z7D9Ar7Rt2ueQ5Vfj4oR24qoAATILnsn8JuLwwoC8N9VKejveSswoA HQBU1wbgsQfZxw9cZX08bV1X5021je1AU58VS6Bx9hoh49pwBiFYFIeFd3mqgnkC AwEAAaNCMEAwHQYDVR00BBYEFOLJQJ9NzuiaoXzPDj9lxSmIahlRMA8GA1UdEwEB /wQFMAMBAf8wDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3DQEBCwUAA4ICAQDRSVfg p8xoWLoBDysZzY2wYUWsEe1jUGn4H3++Fo/9nesLqjJHdtJnJO29fDMylyrHBYZm DRd9FBUb10v9H5r2XpdptxolpAqzkT9fNqyL7FeoPueBihhX0YV0GkLH6VsTX4/5 COmSdI31R9Kr09b7eGZONn356ZLpBN79SWP8bfsUcZNnL0dKt7n/HipzcEYwv1ry L3ml4Y0M2fmyYzeMN2WFcGpcWwlyua1jPLHd+PwyvzeG5LuOmCd+uh8W4XAR8gPf JWIyJyYYMoSf/wA6E7qaTfRPuBRwIrHKK5DOKcFw9C+df/KQHtZa37dG/OaG+svg IHZ6uqbL9XzeYqWxi+7egmaKTjowHz+Ay60nugxe19CxVsp3cbK1daFQqUBDF8Io 2c9SilvIY9RCPqAzekYu9wogRlR+ak8x8YF+QnQ4ZXMn7sZ8uI7XpTrXmKGcjBBV 09tL7ECQ8s1uV9JiDnxXk7Gnbc2dg7sq5+W2O3FYrf3RRbxake5TFW/TRQ11brqQ XR4EzzffHqhmsYzmIGrv/EhOdJhCrylvLmrH+33RZjEizIYAfmaDDELOvTSSwxrq T8p+ck0LcIymSLumoRT2+1hEmRSuqguTaaApJUqlyyvdimYHFngVV3Eb7PVHhPOe MTd61X8kreS8/f3MboPoDKi3QWwH3b08hpcv0g== ----END CERTIFICATE----

2. 查看密钥库文件信息

运行 JDK 所在路径 bin 目录下的 keytool 工具:

参考:

keytool -list -keystore keystore.jks -storepass yourpassword 例:

keytool -list -keystore D:\keystore.jks -storepass 123456







示例私钥的别名(alias)为 testweb,在导入服务器证书时需要使用。导入证书时,一定要使用产生证书请求文件时生成的 keystore.jks 文件。该文件 丢失或用新生成的 keystore.jks 文件都会导致无法正确导入您的服务器证书。

3. 导入证书

导入根证书

参考:

keytool -import -alias root -keystore keystore.jks -trustcacerts -storepass yourpassword -file root.cer

导入 CA 证书

参考:

keytool -import -alias secondary -keystore keystore.jks -trustcacerts -storepass yourpassword -file secondary.cer

例:

导入根证书

keytool -import -alias GDCA_TrustAUTH_R5_ROOT -keystore D:\keystore.jks -trustcacerts -storepass 123456 -file D:\GDCA_TrustAUTH_R5_ROOT.cer 地址: 广州市东风中路 448 号成悦大厦第 23 楼 邮编: 510030 网址: www.gdca.com.cn

电话: 8620-83487228 传真: 8620-83486610 客户服务(热线): 95105813





提示是否信任该证书,填:Y



keytool -import -alias GDCA_TrustAUTH_R4_EV_SSL_CA -keystore D:\keystore.jks -trustcacerts -storepass 123456 -file D:\GDCA_TrustAUTH_R4_EV_SSL_CA.cer

```
c:\java\bin>keytool -import -alias GDCA_TrustAUTH_R4_EV_SSL_CA -keystore D:\keys
tore.jks -trustcacerts -storepass 123456 -file D:\GDCA_TrustAUTH_R4_EV_SSL_CA.ce
r.cer
```

导入服务器证书

参考:

keytool -import -alias yourserver -keystore keystore.jks -trustcacerts -storepass password -file server.cer

例:

keytool -import -alias testweb -keystore D:\keystore.jks -trustcacerts -storepass 123456 -file D:\testweb.gdca.com.cn.cer

c:\Java\jdk1.6.0_45\bin>keytool -import -alias testweb -keystore D:\keystore.jks -trustcacerts -storepass 123456 -file D:\testweb.gdca.com.cn.cer 认证回复已安装在 keystore中

导入服务器证书时,服务器证书的别名和私钥别名必须一致。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"。

另外导入时如果出现报错"invalid DER-encoded certificate data",请参考步骤"1.3转换证书编码"将服务器证书文件保存成 Base64 编码格式,然后重新执行导入操作。

```
c:\Java\jdk1.6.0_45\bin>keytool -import -alias testweb -keystore D:\keystore.jks
-trustcacerts -storepass 123456 -file D:\testweb.cer
keytool错误: java.security.cert.CertificateParsingException: invalid DER-encode
d certificate data
```

证书导入完成,运行 keystool 命令,再次查看 keystore 文件内容 keytool -list -keystore D:\keystore.jks -storepass 123456



4. 产生 truststore 文件(可选):

配置双向 SSL 时需要使用 truststore. jks, 单向 SSL 时可以不使用。

导出凭证文件

参考:

keytool -export -alias testserver -keystore keystore.jks -rfc -file

trustcert.cer -storepass yourpasssword

例:



keytool -export -alias testweb -keystore D:\keystore.jks -rfc -file

D:\trustcert.cer -storepass 123456

c:\Java\jdk1.6.0_45\bin>keytool -export -alias testweb -keystore D:\keystore.jks -rfc -file D:\trustcert.cer -storepass 123456 保存在文件中的认证 <D:\trustcert.cer>

将凭证文件 导入到 truststore 文件

参考:

keytool -import -alias testserver -file trustcert.cer -keystore

truststore.jks -storepass yourpasssword

-keystore 指定生成的 truststore 文件, -storepass 指定 truststore 密码例:

keytool -import -alias testweb -file D:\trustcert.cer -keystore

D:\truststore.jks -storepass 123456

四、安装服务器证书

1. 单向 SSL

1.1 配置服务器

登陆 Weblogic 控制台,点击-环境-服务器:





ORACLE WebLogic Server 管理控制台 12c

更改中心	🍙 主页 注销 首选项 🔤 记录 帮助
查看更改和重新启动	主页 >服务發模徑 >AdminServer > 服务容模 餐
启用配置编辑。将来在修改,添加或删除此 地中的项目时,将自动激行这些更改。	服务器概要
城中的风白明,村自动激着这些更快。	電置 控制
域结构	
testweb 中-城分区 白-环境 服务器 	服务器是 WebLogic Server 的实例, 它运行在自己的 Java 虚拟机 (JVM)上, 此页概括了已在当前 WebLogic Server 域中配置的每一个服务器。
资源组 资源组模板 计算机 虚拟12机	▶ 定制此表 服务器(已新选-更多列存在)
 □ 「虚拟目标 □ 二作管理器 □ 一并发模板 □ 一资源管理 	新建 <u> 京隆</u> 一 名称 ↔
帮助主题 □	AdminServer (管理)
 创建托管服务器 古路服务器 	新建。 克隆 删除

在服务器列表里选择要配置 SSL 证书的服务器

	与守守在此 计中心二分二十	-A- 765	n+lotat		七台コムカ新三里	
労奋走 weblogic server H	9头例,它还171: 	±自己的 東)異的海	Java 虚拟机 、 本丽客 98	(JMM) 上, 卅戶	相目口的版本。	
贝概括了已往当前 WebLo	igic Server 现中	即面的母	一个服务器	•		
自制此表						
官制此表 (齐器 (已篩迭 - 更多列4	テ在)					
注制此表 (齐器 (已筛选 - 更多列4 新建] 克隆] 删除	芊在)			显示 1	到1个,共1个	· 上一个 下·
E 制此表 (六番 (己筛选 - 更多列 杆 新建] 「克隆」 冊除 - 名称 〜	字在) 类型	集群	计算机	显示 1 状态	到1个,共1个 健康状况	 上一个 下・ 监听端口

在 "配置"- "一般信息",可以配置服务器的 http 和 https 是否启用, 以及对应的端口号。webloigc 默认的 https 端口号为 7002,请在选项启用 SSL 并根据实际情况修改端口号:





数安时代科技股份有限公司 Global Digital Cybersecurity Authority Co., Ltd.

配置 协议	(日志	記录	调试	监视	控制	部署	服务	安全	注释			
一般信息	集群	服务	密钥库	SSL	联合	服务	部署	迁移	优化	超载	并发	ĵ.
服务器启动	Web	服务	Coheren	ice								
保存												
使用此页可 查看 JNDI 标	J以配置 _对 @	该服务	器的一般	功能, 例	如默认	网络通	信。					
名称:			Adr	ninServe	er			此服 息…	务器实例	削的字母	数字式:	名利
模板:			(未	指定值)) 更改			用于i	配置此月	勝務器的	模板。	Ē
🋃 计算机:			(无)				将要: (计算	运行此月 (机)。	勝務器的 更多信!	WebLog 킔	gic
🋃 集群:			Сјф	立)				该服 例组	务器所属 。 更多	鷗的集群 ≶信息	,或 Wel	ЬLc
🎸 监听地块	ll:							此服 名。 myma	务器用于 例如,相 achine。	「监听传 应地输」 更多信	入连接的 入 12.34 這息	钓: .5.
☑ 启用监叫	端口							指定: 听端	是否可以 口访问此	人通过默 化服务器	认的纯 。 更	文2 多作
监听端口:			70	001				此服 默认	务器用邦 TCP 端D	k监听常 コ。 更	规 (非 5 多信息,	SL)
☑ 启用 551	监听家							指示: 服务:	是否可以器。 夏	人通过默 更多信息	认的 SS 	LIJ
SSL 监听端	0:		70	102				此服	务器监叫 。 軍 多	f SSL 连 ≶信息	接请求用	䜣仓

1.2 配置认证模式

选择"密钥库",并设置认证方式:

一般信息	集群	服务	密钥库	SSL	联合服务	部署	迁移	Ø
保存			L					
<i>रू धा ह</i> ता।) 726/모크)	右欧铜		0 Z4 240	ቀክ / ረጉል እ ሱስታት	~+***		
DO ANTELI	以明怀型	有雷切	和可居旺士	则没久彻	/141(CA)的安	主任陌祖	れ居住。	വ
	以明不知	有否切	천년] 18 년 구3	·加州友作	.149 (CA) 出)支	主行項1	机局准。	在」
密钥库:	54 MH (* 172	清密研 演示标	和中国证书 识和演示信		改	至1子陌1	¶EI£ ∘	Æ1





Adminserver的反应

沁	日志记录	调试	监视	控制	部署	服务
(1	集群 服务	密制	车 53	5L 联合	服务	部署
动	Web 服务	Cohere	nce			
似消_						
可以确	4保私有密钥:	和可信证	F书领发	复机构 (C#	\) 65æ∢	
医有助	が手管理消息: 「	传输的梦	全。		->20 A V	全存储
	し () 集 転力 取消 可以確	 集群 服务 (試) Web 服务 (取消) (1)) (1)) (4) (4)	! 集群 服务 密钥 」	! 集群 服务 密钥库 SS	! 集群 服务 密钥库 SSL 联合 該加 Web 服务 Coherence 取消	! 集群 服务 密钥库 SSL 联合服务

选择"定制标识和 Java 定制信任"。

将您的密钥库文件 keystore. jks 上传到服务器上,并配置文件路径和密钥 库文件密码:

一般信息	集群	服务	密钥库	SSL	联合服务	部署	迁移	ť
服务器启动	Web	服务	Coherence	1				
保存								
<i>密钥库</i> 可以 置。这些设	确保私 置有助	有密钥 于管理	和可信证书; 消息传输的;	颁发机 安全。	,构 (CA) 的安	全存储和	喧理。	在
密钥库:			定制标	识和:	lava 标准信任	E更改	1	查抄
- 标识								
🛃 定制标识	、密钥 周	车 :	D:\ss	l\key:	store.jks		4 14 14	标还和库
🕢 定制标识	(密钥)	车类型 :	jks					容是3000000000000000000000000000000000000
定制标识密	铺库密			•••			in term	定常信
确认定制标i 语:	识密制	库密码	短 ••••	•••				

配置 JRE 默认信任库文件 cacerts。cacerts 默认密码为 changeit。





— 信任 ————		
Java 标准信任密钥库:	C:\Java\JDK18~1.0_6 \jre\lib\security\cacerts	Ja
Java 标准信任密钥库类型:	jks	Ja JK
Java 标准信任密钥库密码 短语:	·····	Ja X
确认 Java 标准信任密钥库 密码短语:	••••••	
保存		

1.3 配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。

输入私钥别名"testweb",并输入私钥密码。

标识和信任位置:	密钥库更改
- 标识	
私有密钥位置:	来自定制标识密钥库
修] 私有密钥别名:	testweb
🎼 私有密钥密码短语:	
🎼 确认私有密钥密码短语:	

1.4 https 访问测试

完成所有配置后,重启 weblogic 服务,就可以立即通过您设定的 SSL 端口 号,访问 https://yourdomain:port 测试 SSL 证书是否安装成功了。



2. 双向 SSL

2.1 配置服务器

登陆 Weblogic 控制台,点击-环境-服务器:

ORACLE WebLogic Server 管理控制台 12c 🏠 主页 注销 首选项 🔤 记录 帮助 Q 更改中心 主页 >服务器模型 >AdminServer > 服务器模要 查看更改和重新启动 启用配置编辑。将来在修改,添加或删除此 域中的项目时,将自动激活这些更改。 服务器概要 配置 控制 域结构 testweb 服务器是 WebLogic Server 的实例, 它运行在自己的 Java 虚拟机 (JVM)上, 由-域分区 白环境 此页概括了已在当前 WebLogic Server 域中配置的每一个服务器。 服务器 **康**万 + 集群 \$5 -Coherence 集群 资源组 ▶ 定制此表 资源组模板 计算机 服务器(已筛选-更多列存在) 虚拟主机 虚拟目标 新建克隆删除 工作管理器 并发模板 □ 名称 ∾ 资源管理 ☐ AdminServer (管理) 帮助主题 Ξ 新建 克隆 删除 • 创建托管服务器 • 古降服条哭

在服务器列表里选择要配置 SSL 证书的服务器

		24-07-0-07-07-07-07-07-07-07-07-07-07-07-0	2010233	10 - 10 - 10 - 10 - 10 - 10 - 10 - 10 -		
务器是 WebLogic Server	的实例, 它运行	在自己的	Java 虚拟机	(JVM)上,并具	有自己的配置。	
页概括了已在当前 Web	Logic Server 掝中	中配置的每	一个服务器	•		
the state of the s						
E朝武表						
E 利耳表 (合箭选 - 更多列	存在)					
E♥ III. 表 务器 (已筛选 - 更多 列 新建 克隆 冊除	存在)			显示 1	到1个,共1个	上一个 下-
E ♥III.表 务器 (已篩迭 - 更多列 新建] 「克隆] 「删除] 名称 ◇]存在) 类型	集群	计算机	显示 1 状态	到1个,共1个 健康状况	上一个 下-

在 "配置"- "一般信息",可以配置服务器的 http 和 https 是否启用, 以及对应的端口号。webloigc 默认的 https 端口号为 7002,请在选项启用 SSL 并根据实际情况修改端口号:



GDCA 信鉴易® SSL 服务器证书部署指南 For Weblogic 12

配置	协议	日志	记录	调试	监视	控制	部署	服务	安全	注释			
一般(言息	集群	服务	密钥库	SSL	联合	服务	部署	迁移	优化	超载	并发	ſ
服务署	器启动	Web	服务	Coheren	ice								
保存													
使用. 查看	此页可 JNDI 科	以配置 对 [@]	该服务	器的一般	功能, 例	如默认	网络通	信。					
名称:				Adr	ninServe	er			此服: 息…	务器实例	帕字母	数字式	名利
模板:				(未	指定值)	更改			用于i	配置此朋	骄器的	模板。	Ē
<u>6</u> ि भे	算机:			(无)				将要; (计算	运行此刖 〔机〕。	勝務器的 更多信!	l WebLo	gic
₫ 集	# :			Qa	立)				该服: 例组	务器所属 。 更多	帥集賴 信息…	,或 We	:bLc
6日 🖞	听地却	t:							此服 名。1 myma	务器用于 例如, 相 achine。	一监听传 应地输 更多作	入连接 入12.34 1息 …	的: 5.
☑ 启	用监听	诸口							指定: 听端	是否可じ 口访问止	し通过駅 と服务器	认的纯 。 更	文2 多信
监听舅	≝ □:			70	001				此服务器用来监听常规 (非 55 默认 TCP 端口 。 更多信息				
☑启	用 SSL	监听舅							指示: 服务;	是否可以 器。 更	し通过割 「多信息	认的 55 	5L ¦
SSL 🖁	浙 瑞	□:		70)02				此服	务器监听 。 更多	f SSL 连 信息	接请求	所他

2.2 配置认证模式

选择"密钥库",并设置认证方式:

一般信息	集群	服务	密钥库	SSL	联合服务	部署	迁移	仂
保存								
密钥库可以	以确保私	有密钥	和可信证书	颁发机	പ构 (CA) 的安	全存储利	喧锂。	在此
密钥库:		演示标	识和演示信	任更	改			
— 标识 —				11	- 19			





保存 取消 <i>密钥库</i> 可以确保私有密钥和可信证书颁发机构(CA)的安全存储和管 密钥库:	迁移	₿
<i>密钥库</i> 可以确保私有密钥和可信证书颁发机构 (CA) 的安全存储和管 密钥库:		
密钥库:	管理。	储和'

选择"定制标识和定制信任"。

将您的密钥库文件 keystore.jks、信任密钥库文件 truststore.jks 上传到 服务器上,并配置文件路径和密钥库文件密码:

密钥库:	定制标识和定制信任更改
- 标识	
④ 定制标识密钥库 :	D:\ssl\keystore.jks
🥵 定制标识密钥库类型:	jks
定制标识密钥库密码短语:	•••••
确认定制标识密钥库密码短语 :	•••••
- 信任	
😰 定制信任密钥库:	D:\ssl\truststore.jks
9 定制信任密钥库类型:	jks
定制信任密钥库密码短语:	
确认定制信任密钥库密码短语 :	•••••
保存	

2.3 配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 -1ist 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。



输入私钥别名"testweb",并输入私钥密码。

🤁 标识和信任位置:	密钥库更改	
- 标识		
私有密钥位置:	来自定制标识密钥库	
6 日 私有密钥别名:	testweb	
修 私有密钥密码短语:	•••••	
6] 确认私有密钥密码短语:	•••••	
证书位置:	来自定制标识密钥库	
- 信任		
可信证书颁发机构:	来自定制信任密钥库	
- ▶ 高级		

点击高级在双向客户机证书行为选择"请求客户机证书并强制使用"

回信证书颁发机构: ▽高级	来自定制信任密钥库	
<u>修</u> 主机名验证:	BEA 主机名验证器 ▼	
<u>d</u> 层 定制主机名验证器:		
导出密钥寿命:	500	
□ 使用服务器证书		
双向客户机证书行为:	请求客户机证书并强制使用	
修] 证书验证者:		

2.4 https 访问测试

完成所有配置后,重启 weblogic 服务,就可以立即通过您设定的 SSL 端口 号,访问 https://yourdomain:port 测试 SSL 证书是否安装成功了。

五、备份和恢复

在您完成服务器证书的安装与配置后,请务必要备份好您的服务器证书,避 免证书遗失给您造成不便:



1. 备份服务器证书

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。如果使用了 truststore,请将 truststore. jks 文件一同备份好。

2. 恢复服务器证书

请参照服务器证书安装部分,重复3.1或3.2即可。

六、证书遗失处理

若您的证书文件损坏或者丢失且没有证书的备份文件,请联系 GDCA (客服热线 95105813)办理遗失补办业务,重新签发服务器证书。

