



广东省数字证书认证中心

GDCA 信鉴易® SSL 服务器证书部署指南

For Weblogic 10 and 11 版本

2015/11/23

目录

一、部署前特别说明.....	2
二、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.....	4
1. 获取服务器证书的根证书和 CA 证书.....	4
1.1 从邮件中获取.....	4
1.2 从 GDCA 官网上下载:	5
1.3 转换证书编码.....	7
2. 查看密钥库文件信息.....	10
3. 导入证书.....	11
4. 产生 truststore 文件(可选):	13
四、安装服务器证书.....	14
1. 单向 SSL	14
1.1 配置服务器	14
1.2 配置认证模式	16
1.3 配置服务器证书私钥别名	17
1.4 https 访问测试	18
2. 双向 SSL	18
2.1 配置服务器	18
2.2 配置认证模式	19
2.3 配置服务器证书私钥别名	20
2.4 https 访问测试	22
五、备份和恢复.....	22
1. 备份服务器证书.....	22
2. 恢复服务器证书.....	22
六、证书遗失处理.....	22



一、部署前特别说明

1. 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
2. 本部署指南适用于 weblogic 10、11 版本;
3. 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, 但地址栏不变绿色;
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。

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 (广东数字证书认证中心有限公司或 Guangdong Certification 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)

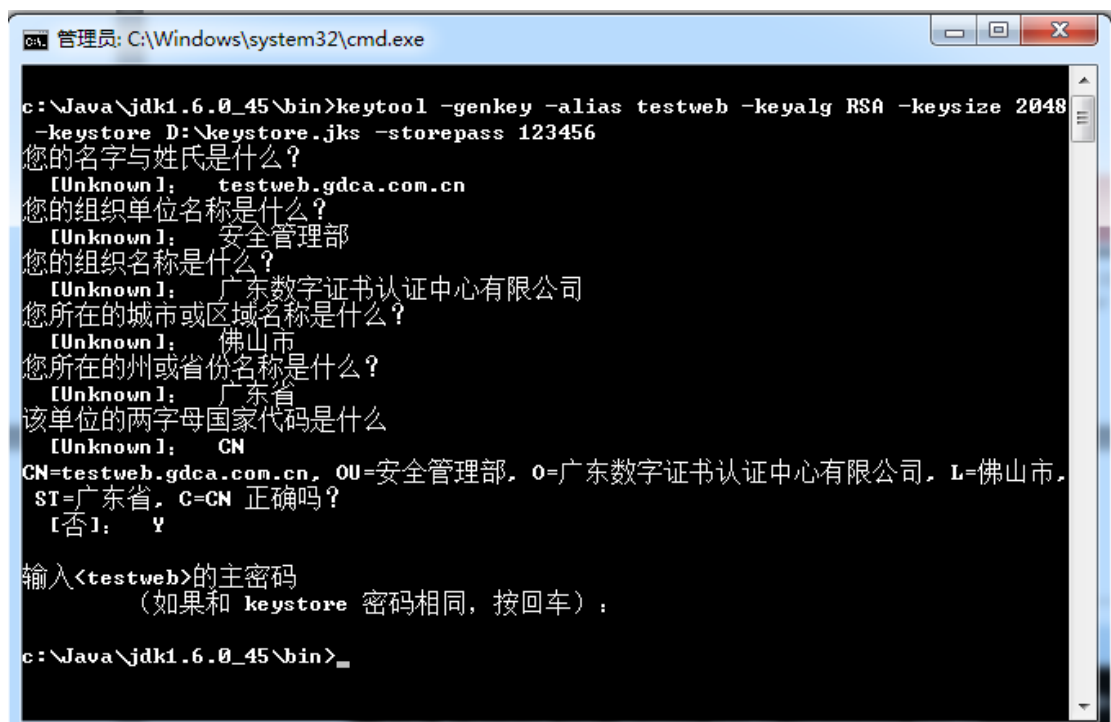
6 该单位的两字母国家代码是什么?

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
```



```
管理员: C:\Windows\system32\cmd.exe
c:\Java\jdk1.6.0_45\bin>keytool -genkey -alias testweb -keyalg RSA -keysize 2048
-keystore D:\keystore.jks -storepass 123456
您的名字与姓氏是什么?
[Unknown]: testweb.gdca.com.cn
您的组织单位名称是什么?
[Unknown]: 安全管理部
您的组织名称是什么?
[Unknown]: 广东数字证书认证中心有限公司
您所在的城市或区域名称是什么?
[Unknown]: 佛山市
您所在的州或省份名称是什么?
[Unknown]: 广东省
该单位的两字母国家代码是什么?
[Unknown]: CN
CN=testweb.gdca.com.cn, OU=安全管理部, O=广东数字证书认证中心有限公司, L=佛山市,
ST=广东省, C=CN 正确吗?
[否]: Y
输入<testweb>的主密码
(如果和 keystore 密码相同, 按回车):
c:\Java\jdk1.6.0_45\bin>
```



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）。

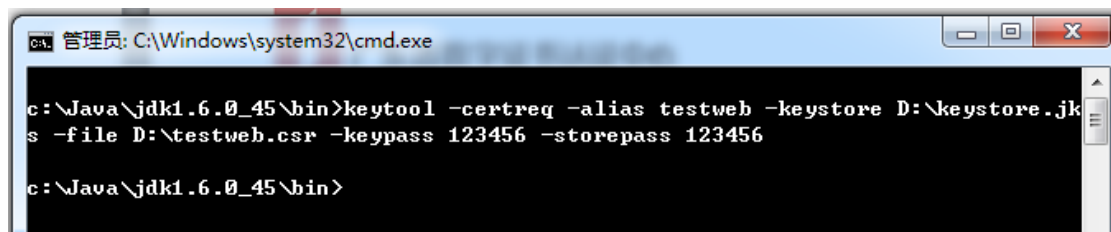
3. 产生证书请求文件

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
```



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。

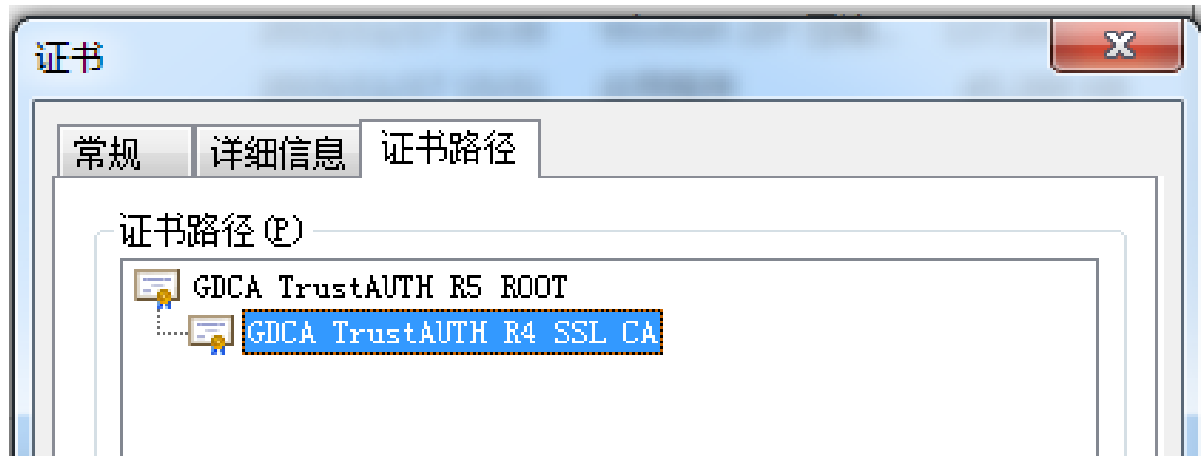
1.1 从邮件中获取

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),

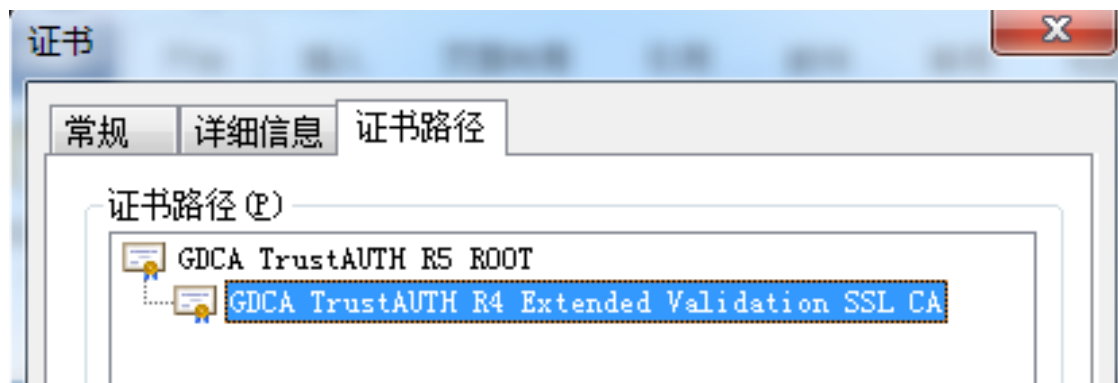


CA 证书就是文件就是 GDCA_TrustAUTH_R4_SSL_CA.cer；如果您申请的是恒信企业 EV SSL 证书 (Extended Validation SSL Certificate)，CA 证书就是文件就是 GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer, 请确认所收到的证书文件是您需要的 CA 证书。

GDCA_TrustAUTH_R4_SSL_CA.cer:



GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer:



1.2 从 GDCA 官网上下载:

<http://www.gdca.com.cn/channel/001002002>





获取根证书:GDCA_TrustAUTH_R5_ROOT.cer:

下载根证书

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）。

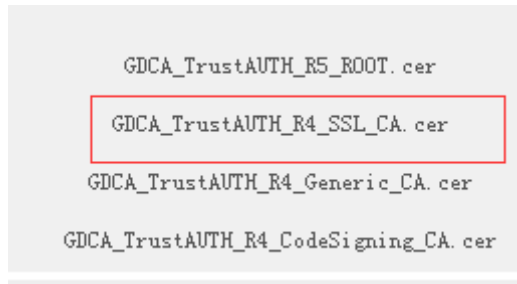
12 项，显示 1 到10. [首页/前一页] 1, 2 [下一页/末页]

CA名称	起始有效时间	截止有效时间	CA证书下载
ROOTCA_sm2	2012-07-14 11:11:59	2042-07-07 11:11:59	社会公众应用根证书 (SM2) .cer
GDCA TrustAUTH E1 CA	2014-06-26 15:02:11	2034-06-21 15:02:11	广东数字证书认证中心有限公司_sm2.cer
ROOTCA_rsa	2005-08-28 16:16:16	2025-08-23 16:16:16	社会公众应用根证书 (RSA) .cer
GDCA TrustAUTH R2 CA	2013-12-16 14:29:40	2018-12-15 14:29:40	广东数字证书认证中心有限公司_rsa.cer
GDCA Root CA	2004-01-11 17:34:22	2024-12-11 00:00:00	GDCA_Root_CA.cer
GDCA Guangdong Certificate Authority	2004-01-12 10:13:07	2024-01-12 10:13:07	GDCA_Guangdong_Certificate_Authority.cer
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 SSL CA	2014-11-26 17:52:00	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_SSL_CA.cer
GDCA TrustAUTH R4 Generic CA	2014-11-26 17:53:00	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2014-11-26 17:54:35	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_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_SSL_CA.cer





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_Extended_Validation_SSL_CA.cer

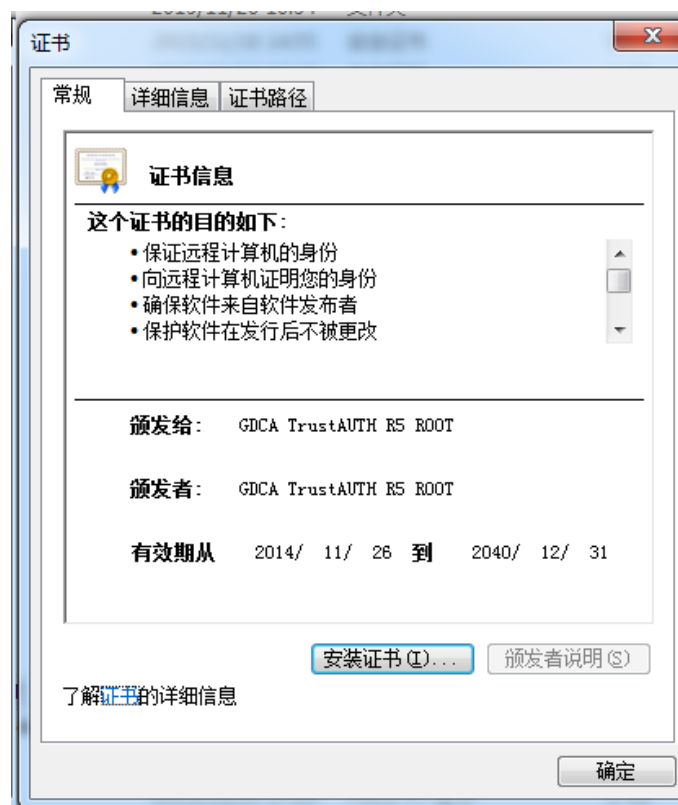
12 项, 显示 11 到12. [首页/前一页] 1, 2 [下一页/末页]

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R4 Extended Validation SSL CA	2014-11-26 17:45:25	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer

1.3 转换证书编码

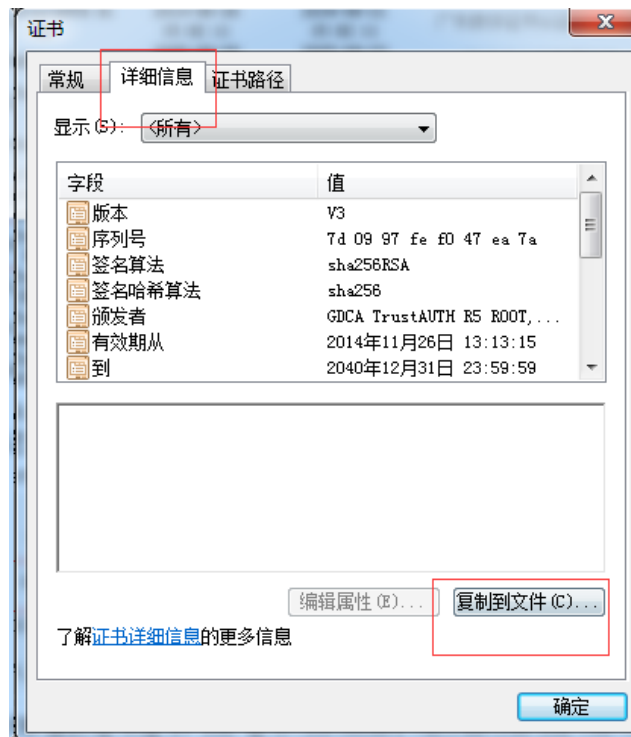
从官网上下载的证书需要先转换为 Base64 编码格式。以根证书为例:

打开证书:



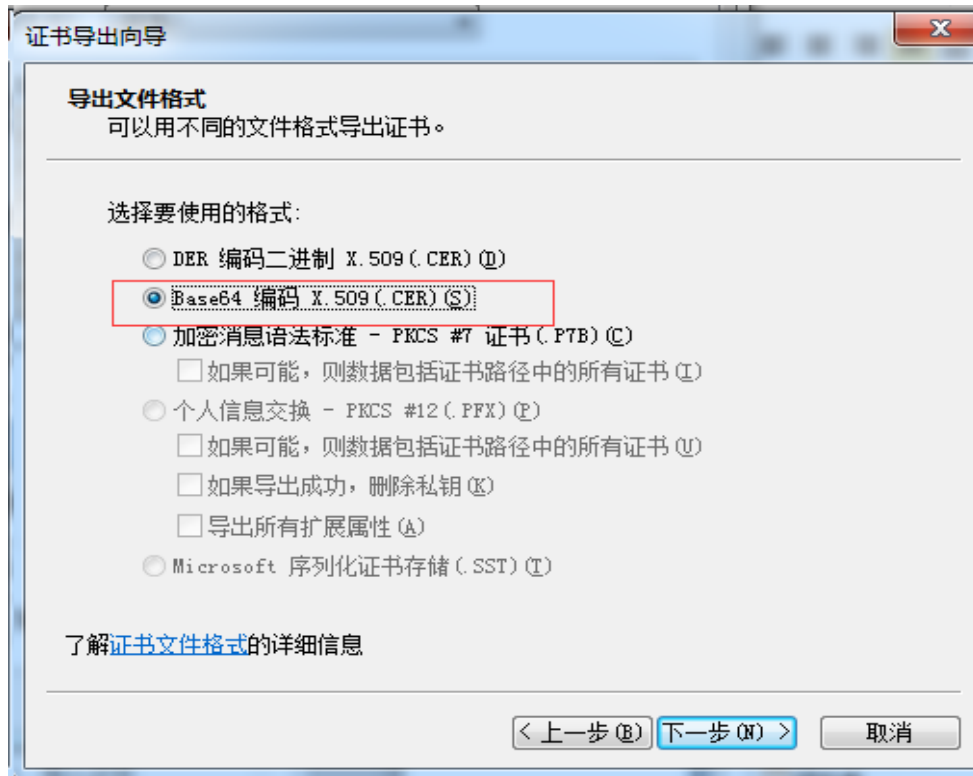
详细信息-复制到文件



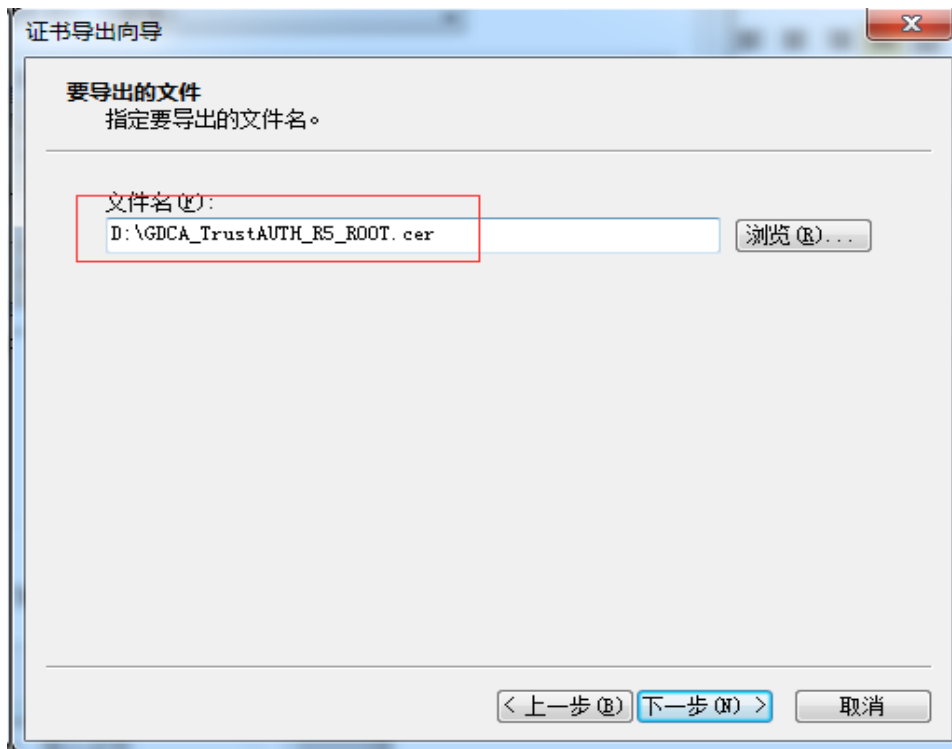


在证书导出向导里，将证书编码改成 Base64 编码格式





导出到指定目录里



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
BhMCQ04xMjAwBGNVBAoMKUDVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVUUSE9SSVRZ
IENPLixMVEQuMR8wHQYDVQDDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMBAQDE0
MTEyNjA1MTMxNVoXDTQwMTIzMTk1OVowYjELMAkGA1UEBhMCQ04xMjAwBGNV
BAoMKUDVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVUUSE9SSVRZIEPLixMVEQuMR8w
HQYDVQDDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMIICiANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCGKCAgEA2aMW8Mh0dHeb7zMNOWZ+Vfy1YI92hhJCfVZmPoiC7XJj
Dp6L3TQsAlFRwxn9WVSEYfFrs0yw6ehGXTjGoqcuEve6ghWinI9tsJlKCVLriXBj
TnnEtlu9o12x8kECK62pOqPseQrsXzrj/e+APK00mxqriCZ7VqKChh/rNYmDf1+u
KU49tm7srsHwJ5uu4/Ts765/94Y9cncrpfTzTqfrlYwiOXnhLQiPzLyRuEH3FMEj
qcOtmkVES7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqWTTQJ9Cy5WmYqsBebnh52nUpm
MUHfP/vFBu8bbtn4arj3ZGM74zkYI+dndRTVdVeSN72+ahsmUPI2JgaQxXABZG12
ZuGR224HwGGALrIuL4xwp9E7PLOR5G62xDtW8mySlwnNR30YwP07ng/Wi64Ht1oP
zgsMR6f1Pri9fcebNaBhlzpbDRfMK5Z3KpIhHtmVdiBnaM8Nvd/WHwLqmuLMC3Gk
L30SgLDTMEZeS1SZD2fJpcjyIMG7J0R38IC+xo70e0gmu9lZJlQDSri3nDxGGeC
jHHeuLzRL5z7D9Ar7Rt2ueQ5Vfj4oR24qoAATILnsn8JuLwwoC8N9VKejveSswaA
HQBUlwBgsQfZxw9cZX08bV1X5O21jeLAU58VS6Bx9hoh49pwBiFYfIeFdmYlrHBYZm
DRd9FBUB10v9H5r2XpdptxolpAqzkt9fNqyL7FeoPueBihhXOYV0GkLH6VsTX4/5
ComSdI31R9Kr09b7eGZONn356ZLpBN79SWP8bfsUcZnL0dKt7n/HipzceYwv1ry
L3ml4YOM2fmyZeMN2WfCgpcWwlyualjPLhd+PwyvzeG5LuOmCd+uh8W4XAR8gPf
JWIyJyYMoSf/wA6E7qaTfRPuBRwIrHKK5DOKcFw9C+df/KQhtZa37dG/OaG+svg
IH26uqbL9XzeYqWxi+7egmaKTjowHz+Ay60nugxe19CxVsp3cbK1daFqQUBDF8Io
2c9SilvIY9RCPgAzekYu9wogR1R+ak8x8YF+QnQ4ZXmn7sZ8uI7XpTrXmKGcjBBV
09tL7ECQ8s1uV9JiDnxXk7Gnbc2dg7sq5+W2O3FYrf3RRbxake5TFW/TRQ11brqQ
XR4EzzfHqhmsYzmIGrv/EhOdJhCrylvLmrH+33RZjEizIYAfmaDDEL0vTSSwXrQ
T8p+ckOLcIymSLumoRT2+lhEmRSugguTaaApJUqlyyvdimYHfngVv3Eb7PVHhPoE
MTd61X8kreS8/f3MboPoDKi3QWwH3b08hpcv0g==
-----END CERTIFICATE-----
```

2. 查看密钥库文件信息

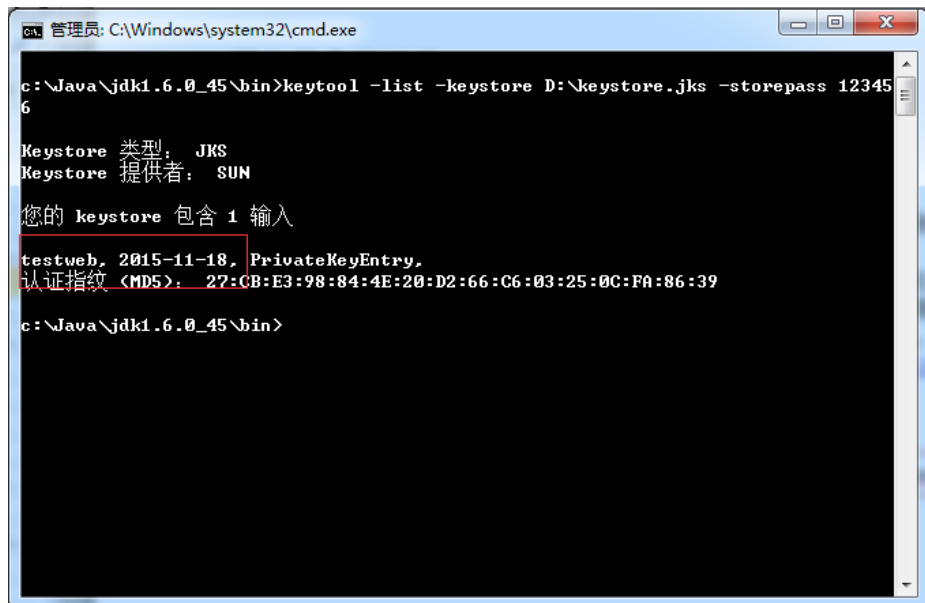
运行 JDK 所在路径 bin 目录下的 keytool 工具。

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

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

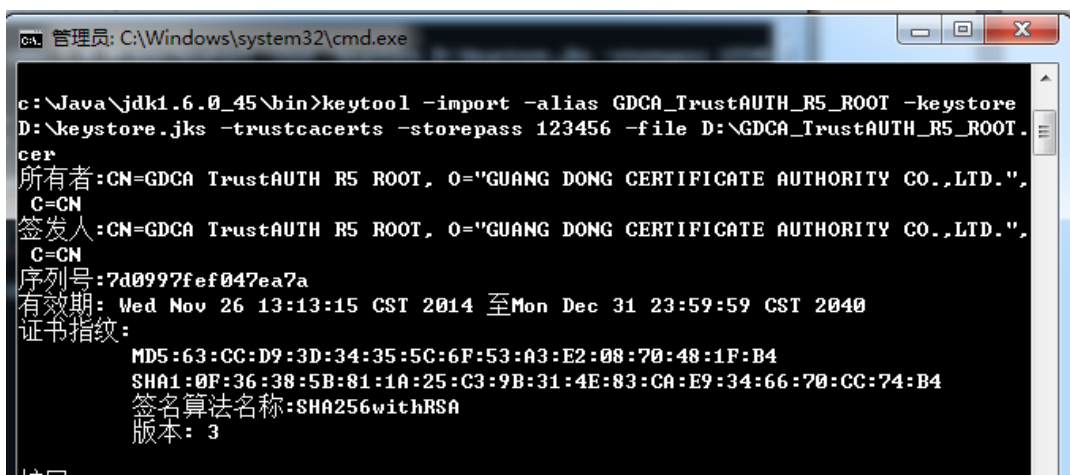
导入 CA 证书

```
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
```



提示是否信任该证书, 填 : Y



```
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E2 C9 40 9F 4D CE E8 9A   A1 7C CF 0E 3F 65 C5 29   ..E.M.....?e.>
0010: 88 6A 19 51                               .j.Q
]
]
信任这个认证? [否]:  Y
认证已添加至keystore中
c:\Java\jdk1.6.0_45\bin>
```

keytool -import -alias GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA
-keystore D:\keystore.jks -trustcacerts -storepass 123456 -file
D:\GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer

```
c:\Java\jdk1.6.0_45\bin>keytool -import -alias GDCA_TrustAUTH_R4_Extended_Valida
tion_SSL_CA -keystore D:\keystore.jks -trustcacerts -storepass 123456 -file D:\G
DCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer
认证已添加至keystore中
```

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，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 keytool 命令，再次查看 keystore 文件内容

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

```
c:\Java\jdk1.6.0_45\bin>keytool -list -keystore D:\keystore.jks -storepass 123456  
6  
Keystore 类型: JKS  
Keystore 提供者: SUN  
您的 keystore 包含 3 输入  
testweb, 2015-11-20, PrivateKeyEntry,  
认证指纹 <MD5>: AC:3F:33:8D:33:73:3A:17:4C:87:04:BC:77:FB:51:99  
gdca_trustauth_r5_root, 2015-11-20, trustedCertEntry,  
认证指纹 <MD5>: 63:CC:D9:3D:34:35:5C:6F:53:A3:E2:08:70:48:1F:B4  
gdca_trustauth_r4_extended_validation_ssl_ca, 2015-11-20, trustedCertEntry,  
认证指纹 <MD5>: 3E:DE:DB:4F:AA:05:02:A2:1C:9A:68:C0:A2:44:C0:DA  
c:\Java\jdk1.6.0_45\bin>
```

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 yourpassword
```

-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
```

```
c:\Java\jdk1.6.0_45\bin>keytool -import -alias testweb -file D:\trustcert.cer -k  
eystore D:\truststore.jks -storepass 123456  
所有者:CN=testweb.gdca.com.cn, OU=安全管理部, O=广东数字证书认证中心有限公司, OI  
D.2.5.4.15=Private, SERIALNUMBER=74709895-8, OID.1.3.6.1.4.1.311.60.2.1.1=佛山市  
, OID.1.3.6.1.4.1.311.60.2.1.2=广东省, OID.1.3.6.1.4.1.311.60.2.1.3=CN, L=佛山市  
, ST=广东省, C=CN  
签发人:CN=GDCA TrustAUTH R4 Extended Validation SSL CA, O="GUANG DONG CERTIFICAT  
E AUTHORITY CO.,LTD.", C=CN  
序列号:6804d4a86c515524  
有效期: Fri Nov 20 09:00:07 CST 2015 至 Sat Nov 19 09:00:07 CST 2016  
证书指纹:  
MD5:AC:3F:33:8D:33:73:3A:17:4C:87:04:BC:77:FB:51:99
```

```
#9: ObjectId: 2.5.29.37 Criticality=false  
ExtendedKeyUsages [  
  serverAuth  
  clientAuth  
]  
信任这个认证? [否]: Y  
认证已添加至 keystore 中
```

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：





在服务器列表里选择要配置 SSL 证书的服务器



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。weblogic 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：

名称: AdminServer

计算机: (None)

集群: (Standalone)

监听地址:

启用监听端口

监听端口:

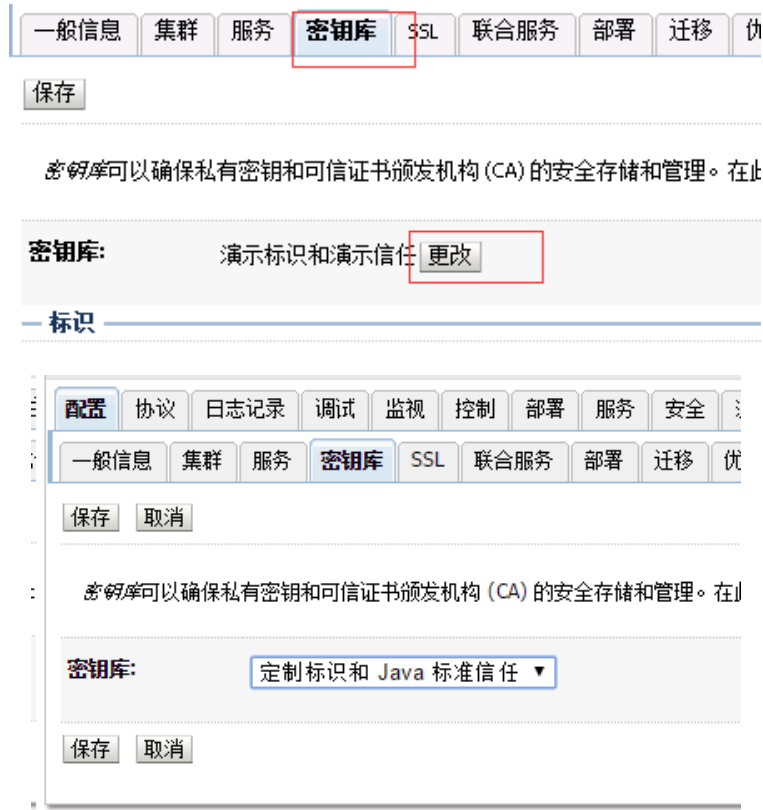
启用 SSL 监听端口

SSL 监听端口:



1.2 配置认证模式

选择“密钥库”，并设置认证方式：



The screenshot shows the configuration interface for the Keystore. The 'Keystore' tab is selected. The 'Keystore' dropdown is set to 'Demo Identity and Demo Trust'. A second screenshot shows the 'Keystore' dropdown set to 'Custom Identity and Java Standard Trust'.

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：



The screenshot shows the configuration interface for the Custom Identity and Java Standard Trust. The 'Custom Identity Keystore' field is set to 'D:\ssl\keystore.jks', the 'Custom Identity Keystore Type' is 'jks', and the 'Custom Identity Keystore Password Phrase' and 'Confirm Custom Identity Keystore Password Phrase' fields are empty.

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



Java 标准信任密钥库:	C:\Java\JDK16~1.0_4\jre\lib\security\cacerts
Java 标准信任密钥库类型:	jks changeit
Java 标准信任密钥库密码短语:
确认 Java 标准信任密钥库密码短语:

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 `keytool -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	
私有密钥位置:	来自定制标识密钥库
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:
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 Java 标准信任密钥库
高级	
<input type="button" value="保存"/>	

点击高级，勾选使用“JSSE SSL”

标识	
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:
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 Java 标准信任密钥库
高级	
<input type="button" value="保存"/>	





The image shows a configuration window for SSL settings. At the top, there is a checkbox labeled '允许未加密的 Null 密码' (Allow unencrypted Null passwords) which is unchecked. Below this are two sections for certificate verification: '进站证书验证:' (Incoming certificate verification) and '出站证书验证:' (Outgoing certificate verification), both with a dropdown menu set to '仅内置 SSL 验证' (Only built-in SSL verification). A red box highlights the '使用 JSSE SSL' (Use JSSE SSL) checkbox, which is checked. At the bottom left, there is a '保存' (Save) button.

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：



在服务器列表里选择要配置 SSL 证书的服务器





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：

名称: AdminServer

计算机: (None)

集群: (Standalone)

监听地址:

启用监听端口

监听端口:

启用 SSL 监听端口

SSL 监听端口:

2.2 配置认证模式

选择“密钥库”，并设置认证方式：

密钥库可以确保私有密钥和可信证书颁发机构 (CA) 的安全存储和管理。在此

密钥库: 演示标识和演示信任

— 标识 —



一般信息 集群 服务 密钥库 SSL 联合服务 部署 迁移 优化 超靴

保存 取消

密钥库可以确保私有密钥和可信证书颁发机构 (CA) 的安全存储和管理。在此页中, 您

密钥库: 定制标识和定制信任

保存 取消

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

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

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 -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

私有密钥位置: 来自定制标识密钥库

私有密钥别名:

私有密钥密码短语:

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 Java 标准信任密钥库

高级

保存

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”，并勾选使用“JSSE SSL”

高级

主机名验证: BEA 主机名验证器 ▼

定制主机名验证器:

导出密钥寿命:

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** ▼

证书验证者:

启用 SSL 拒绝日志记录

允许未加密的 Null 密码

入站证书验证: 仅内置 SSL 验证 ▼

出站证书验证: 仅内置 SSL 验证 ▼

使用 JSSE SSL



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。

