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

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.....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
六、证书遗失处理.....24

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 12 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）

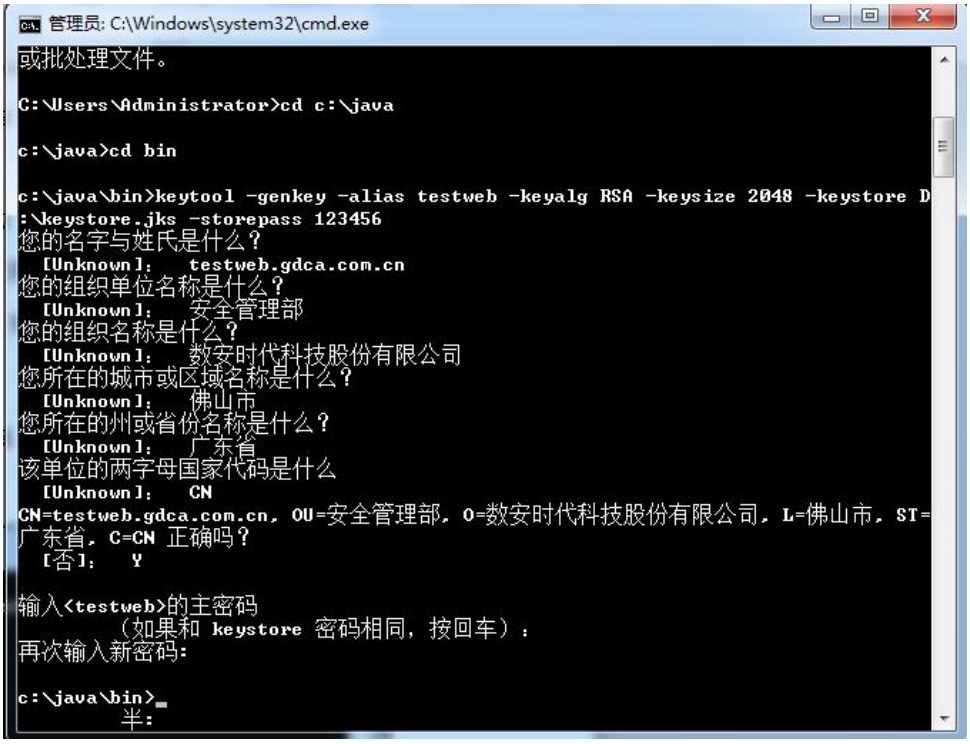
6 该单位的两字母国家代码是什么？

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

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

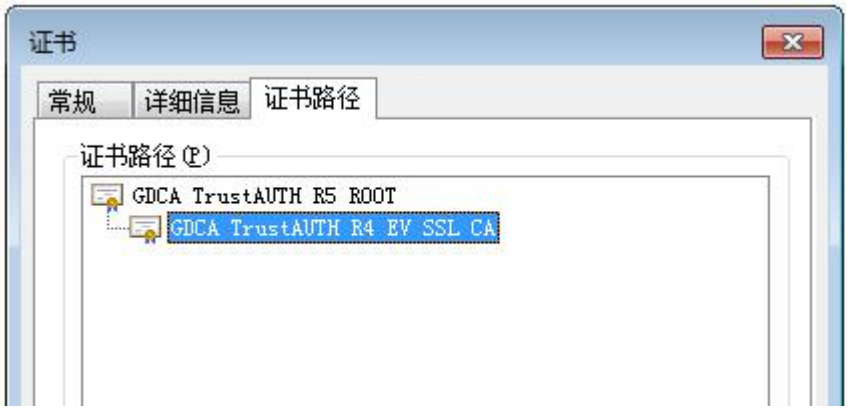
服务器证书需要安装根证书和 CA 证书，以确保证书在浏览器中的兼容性。有两种方式获取。

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）

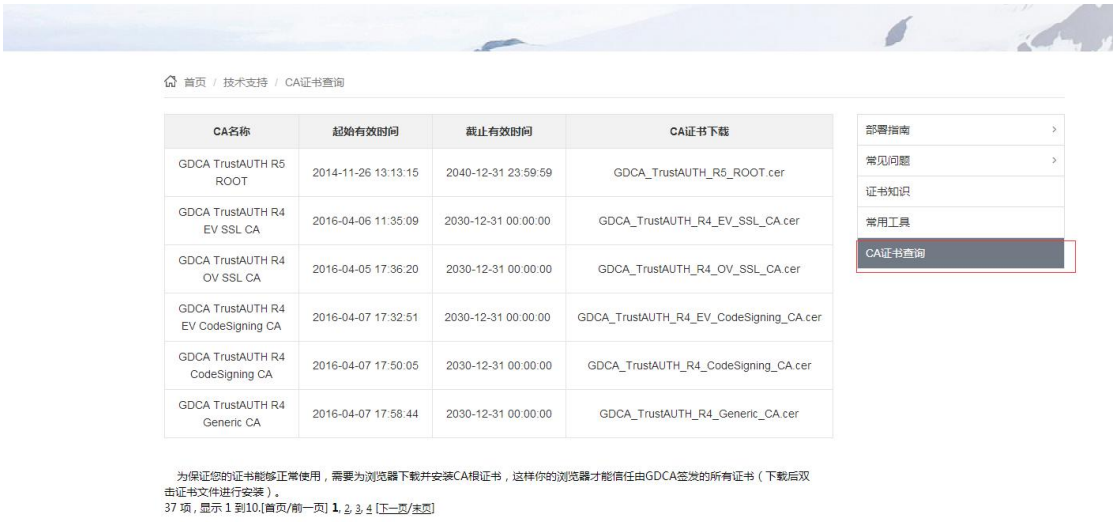
GDCA_TrustAUTH_R4_OV_SSL_CA.cer：

GDCA_TrustAUTH_R4_EV_SSL_CA.cer：



1.2 从 GDCA 官网上下载：

https://www.trustauth.cn/support/ca_cq/



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

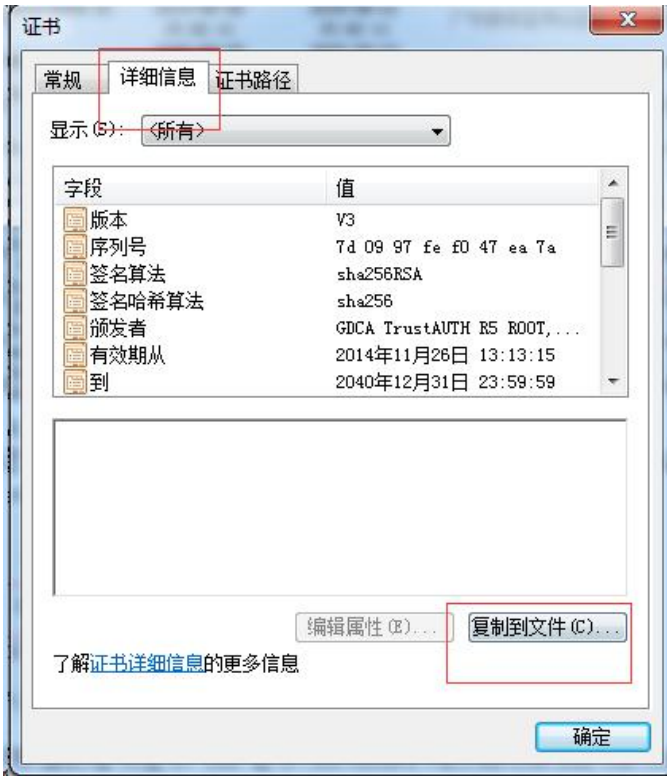
为保证您的证书能够正常使用，需要为浏览器下载并安装CA根证书，这样你的浏览器才能信任由GDCA签发的所有证书（下载后双击证书文件进行安装）。
37 项，显示 1 到10.[首页/前一页] **1**, 2, 3, 4 [下一页/末页]

1.3 转换证书编码

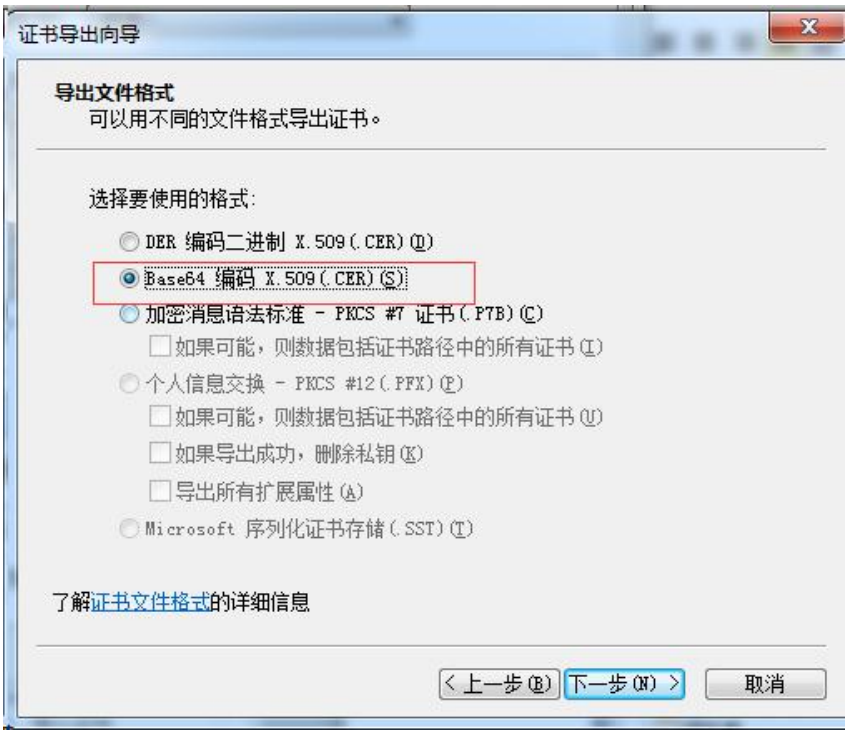
从官网上下载的证书需要先转换为 Base64 编码格式。以根证书为例：

打开证书：

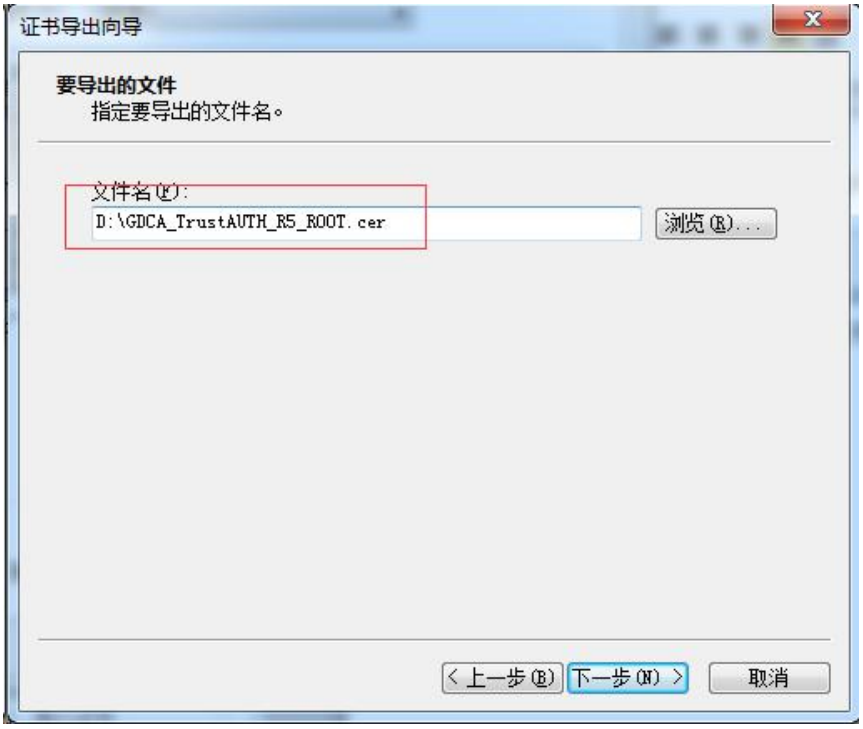
详细信息-复制到文件



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
BhMCQ04xMjAwBgNVBAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZ
IENPLixMVEQuMR8wHQYDVQQDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMB4XDTE0
MTEyNjA1MTMxNVoXDTQwMTIzMTE1NTk1OVowYjELMAkGA1UEBhMCQ04xMjAwBgNV
BAoMKUdVQU5HIERPTkcgQ0VSVElGSUNBVEUgQVVUSE9SSVRZIENPLixMVEQuMR8w
HQYDVQQDDBZHRENBIFRydXN0QVVUSCBSNSBST09UMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEA2aMW8Mh0dHeb7zMNOwZ+Vfy1YI92hhJCfVZmPoiC7XJj
Dp6L3TQsAlFRwxn9WVSEyfFrs0yw6ehGXTjGoqcuEVe6ghWinI9tsJlKCvLriXBj
TnnEt1u9ol2x8kECK62pOqPseQrsXzrj/e+APK00mxqriCZ7VqKChh/rNYmDf1+u
KU49tm7srsHwJ5uu4/Ts765/94Y9cnrrpftZTqfrlYwiOXnhLQiPzLyRuEH3FMEj
qcOtmkVEs7LXLM3GKeJQEK5cy4KOFxg2fZfmiJqwTTQJ9Cy5WmYqsBebnh52nUpm
MUHfP/vFBu8btn4aRjb3ZGM74zkYI+dndRTVdVeSN72+ahsmUPI2JgaQxXABZG12
ZuGR224HwGGALrIuL4xwp9E7PLOR5G62xDtw8mySlwnNR30YwPO7ng/Wi64HtloP
zgsMR6flPri9fcebNaBhlzpBdRfMK5Z3KpIhHtmVdiBnaM8Nvd/WHwlqmuLMc3Gk
L30SgLdTMEZeS1SZD2fJpcjyIMGC7J0R38IC+xo70e0gmu9lZJIQDSri3nDxGGeC
jGHeuLzRL5z7D9Ar7Rt2ueQ5Vfj4oR24qoAATILnsn8JuLwwoC8N9VKejveSswoA
HQBUlwbgsQfZxw9cZX08bVlX5O2ljelAU58VS6Bx9hoh49pwBiFYFIeFd3mqgnkC
AwEAAaNCMEAwHQYDVR0OBBYEFOLJQJ9NzuiaoXzPDj9lxSmIahlRMA8GA1UdEwEB
/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3DQEBCwUAA4ICAQDRSVfg
p8xoWLoBDysZzY2wYUWsEe1jUGn4H3++Fo/9nesLqjJHdtJnJO29fDMylyrHBYZm
DRd9FBUb1Ov9H5r2XpdptxolpAqzkT9fNqyL7FeoPueBihhXOYV0GkLH6VsTX4/5
COmSdI31R9KrO9b7eGZONn356ZLpBN79SWP8bfsUcZNnL0dKt7n/HipzcEYwv1ry
L3ml4Y0M2fmyYzeMN2WFcGpcWwlyua1jPLHd+PwyvzeG5LuOmCd+uh8W4XAR8gPf
JWIyJyYYMoSf/wA6E7qaTfRPuBRwIrHKK5DOKcFw9C+df/KQHtZa37dG/OaG+svg
IHZ6uqbL9XzeYqWxi+7egmaKTjowHz+Ay60nugxe19CxVsp3cbK1daFQqUBDF8Io
2c9Si1vIY9RCPqAzekYu9wogRlR+ak8x8YF+QnQ4ZXMn7sZ8uI7XpTrXmKGcjBBV
09tL7ECQ8s1uV9JiDnxXk7Gnbc2dg7sq5+W2O3FYrf3RRbxake5TFW/TRQl1brqQ
XR4EzzffHqhmsYzmIGrv/EhOdJhCrylvLmrH+33RZjEizIYAfmaDDEL0vTSSwxrq
T8p+ck0LcIymSLumoRT2+1hEmRSuqguTaaApJUq1yyvdimYHFngVV3Eb7PVHhPOe
MTd61X8kreS8/f3MboPoDKi3QWwH3b08hpcv0g==
-----END CERTIFICATE-----
```

2. 查看密钥库文件信息

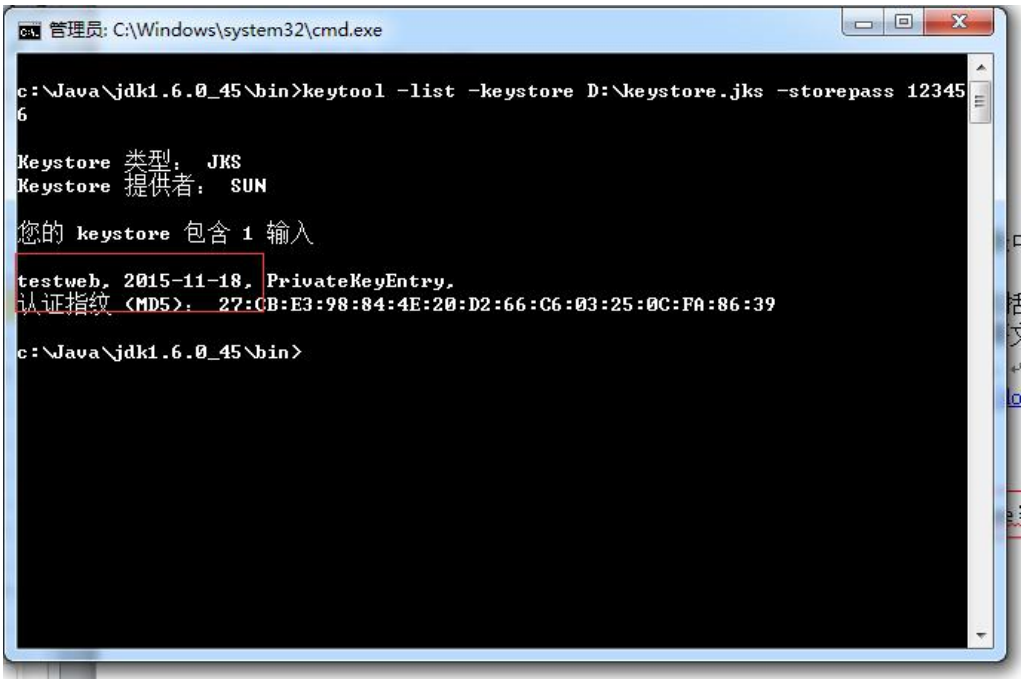
运行 JDK 所在路径 bin 目录下的 keytool 工具：

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

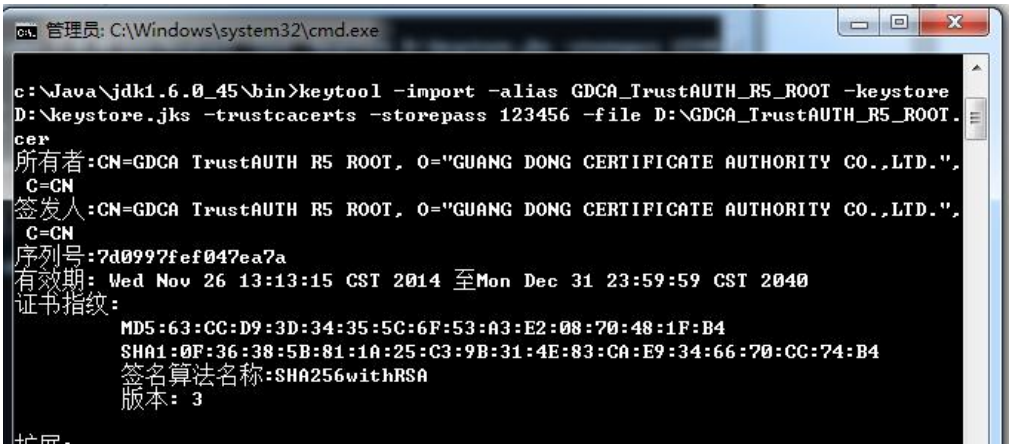
参考：

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

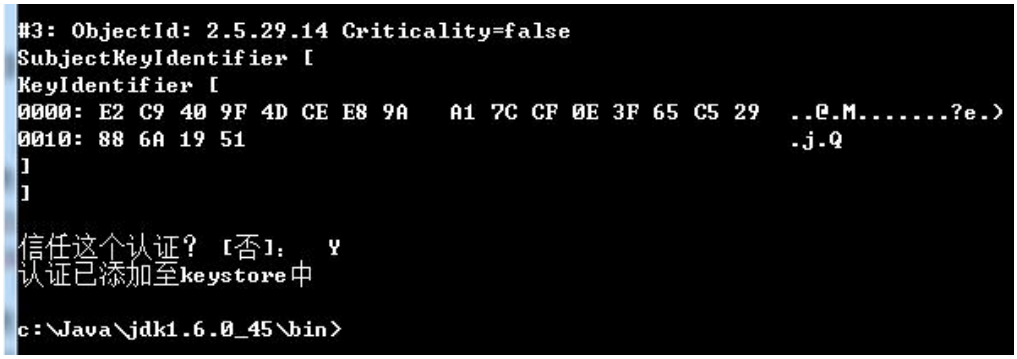
例：

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



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

导入服务器证书

参考：

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

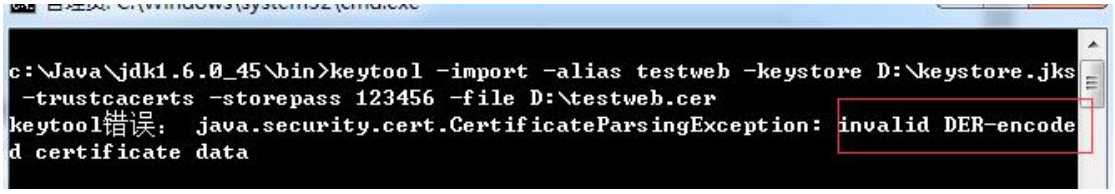
例：

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

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

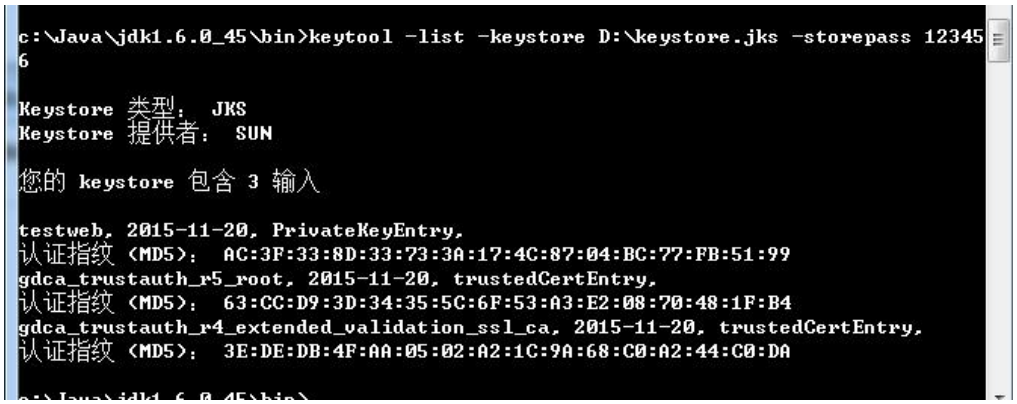
级 CA 证书和导入服务器证书时的提示信息，如果您在导入服务器证书时使用的别名与私钥别名不一致，将提示“认证已添加至 keystore 中”而不是应有的“认证回复已安装在 keystore 中”。

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。



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

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：

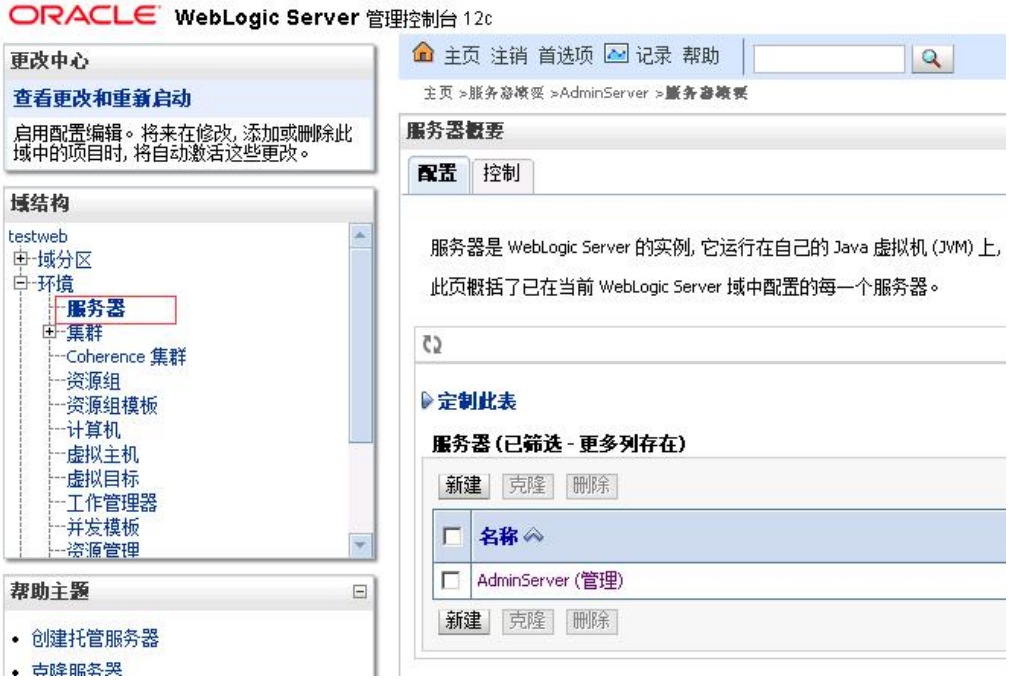
keytool -import -alias testweb -file D:\trustcert.cer -keystore D:\truststore.jks -storepass 123456

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：



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：

1.2 配置认证模式

选择“密钥库”，并设置认证方式：

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：

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

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。

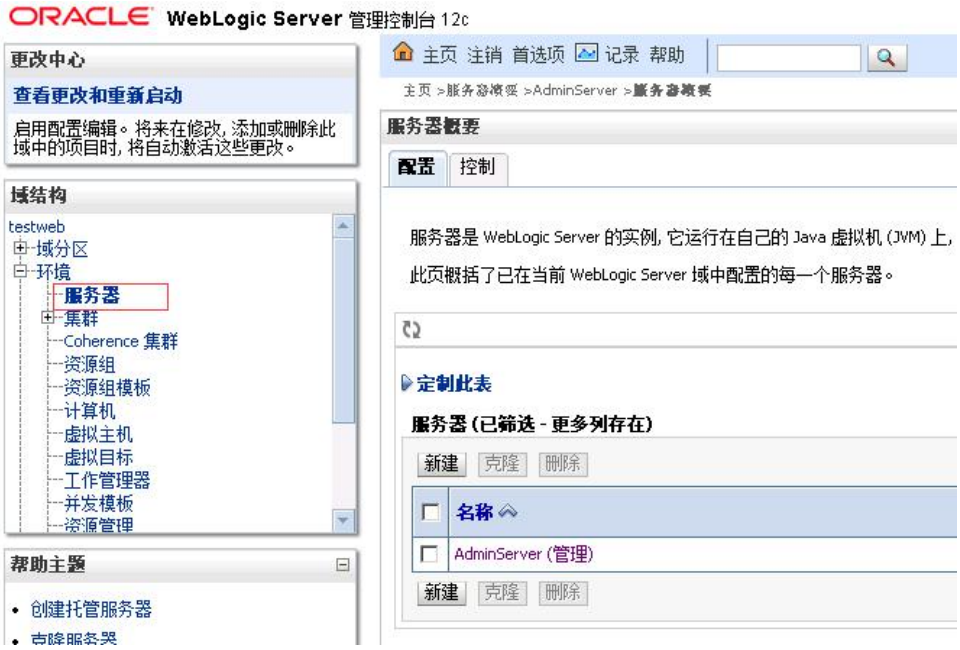
1.4 https 访问测试

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

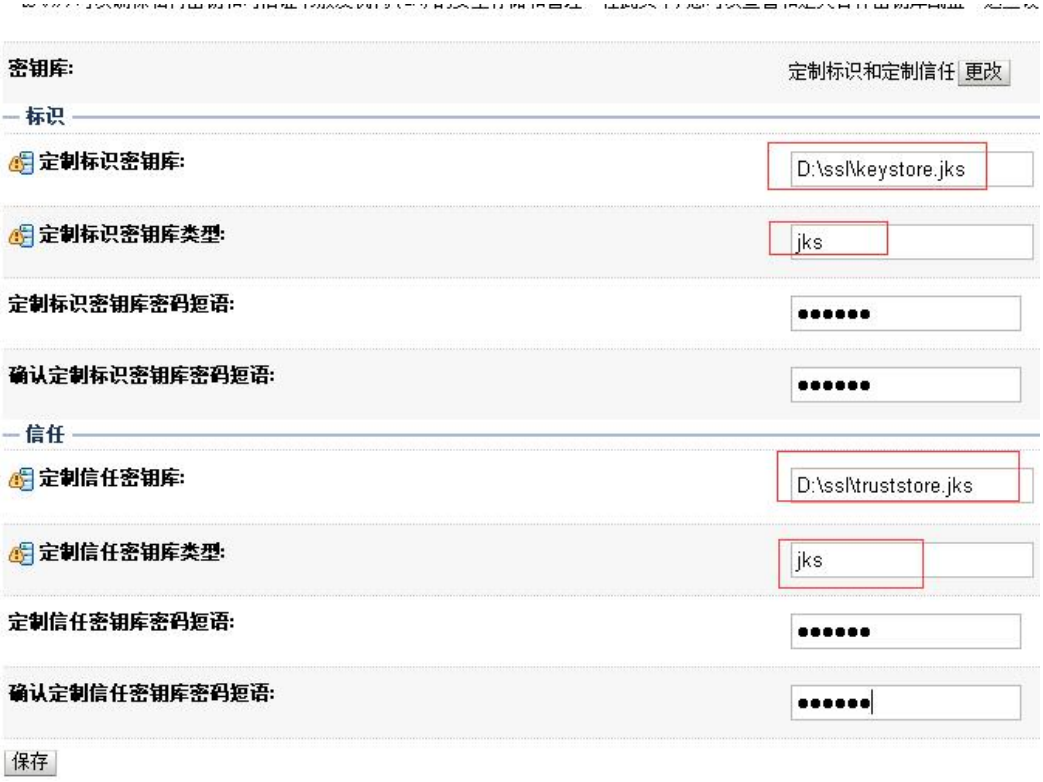
在 “配置”- “一般信息”，可以配置服务器的 http 和 https 是否启用，以及对应的端口号。webloigc 默认的 https 端口号为 7002，请在选项启用 SSL 并根据实际情况修改端口号：

2.2 配置认证模式

选择“密钥库”，并设置认证方式：

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：



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。

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”

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。