



最后更新时间: 2010年12月7日

软件版本号: windows xp sp3  
weblogic server 9.2 jdk1.5

服务器证书安装配置指南系列之  
weblogic 服务器证书安装配置指南

[www.cnnic.cn](http://www.cnnic.cn)

中国互联网络信息中心 (CNNIC)

地址: 北京中关村南四街四号中国科学院软件园1号楼一层

7\*24小时客户服务咨询电话: 86-10-58813000

传真: 86-10-58812666

邮政地址: 北京349信箱6分箱 CNNIC

邮政编码: 100190

## 目录

1. 关于 Weblogic.....	3
2. 生成证书请求文件CSR.....	4
2.1 生成私钥 .....	4
2.2 生成CSR.....	6
2.3 备份私钥文件.....	6
2.4 把CSR发给CNNIC.....	7
3. 下载服务器证书.....	7
3.1 准备下载服务器证书所需信息.....	7
3.2 下载证书.....	7
4. 安装跟证书和服务证书.....	12
4.1 下载根证书及CNNIC中级根证书.....	12
4.2 将根证书root.cer导入到keystore文件.....	12
4.3 将中级CA证书cnnic.cer导入到keystore文件.....	13
4.4 将服务器证书m1.cnnic.cn.cer导入到keystore文件.....	13
4.5 查看keystore证书.....	14
5. 配置weblogic.....	15
6. 完成配置.....	17

## 图表目录

图表一创建私钥.....	5
表二生成 csr 文件.....	6
图表三查看 csr 文件.....	6
图表四可信服务器证书下载页面.....	8
图表五填入收到的参考号和授权码以及生成的 csr.....	9
图表六生成证书.....	10
图表七格式转换.....	11
图表八证书导出向导.....	12
图表九导入根证书.....	13

图表十导入中级根证书.....	13
图表十一导入服务器证书.....	14
图表十二查看 keystore 证书.....	14
图表十三 修改配置一.....	15
图表十四 修改配置二.....	16
图表十五 修改配置三.....	17
图表十六 安装成功后显示服务器证书.....	18

## 1. 关于 Weblogic

本文示例使用的是 Windows 系统下的 weblogicserver9.2, 如果进行 Weblogic 配置时不能成功完成, 可能是版本原因, 请参考 Weblogic 帮助文件中 SSL 相关章节或咨询 Weblogic 服务提供商进行配置。

本文使用“keytool”来生成私钥和 CSR 文件, JDK 中一般已经默认安装有 keytool, 如果您的服务器上没有安装 keytool, 请先下载安装 JDK。

## 2. 生成证书请求文件 CSR

### 重要注意事项

在生成 CSR 文件时同时生成您的私钥, 如果您丢了私钥或忘了私钥密码, 则颁发证书给您后不能安装成功! 您必须重新生成私钥和 CSR 文件, 利用证书补办流程颁发新的证书。为了避免此情况的发生, 请在生成 CSR 后一定要备份私钥文件和记住私钥密码, 最好是在收到证书之前不要再动服务器

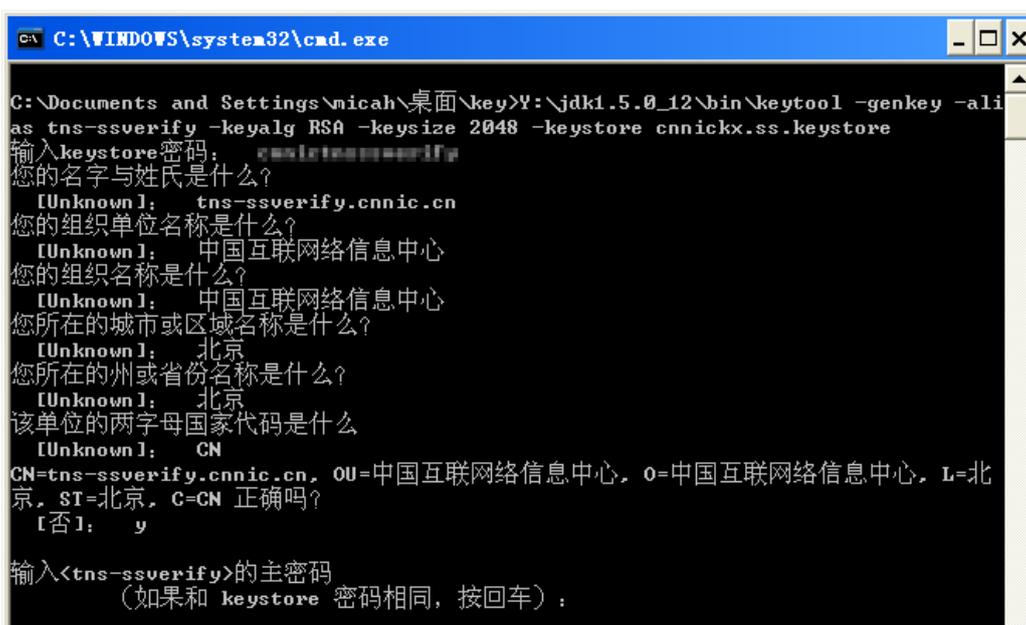
### 1) 生成keystore和keyEntry

请使用以下命令, 并参考下图:

```
Keytool -genkey -alias [keyEntry_name] -keyalgRSA -keysize 2048  
-keystore [keystore_name]
```

注: []中的内容为需要输入的参数, 以上命令间都有空格

- keyEntry\_name: 表示证书的别名
- keystore\_name: 表示证书密钥库的文件名, 扩展名一般为 keystore



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\micah\桌面\key>Y:\jdk1.5.0_12\bin\keytool -genkey -alias tns-ssverify -keyalg RSA -keysize 2048 -keystore cnnickx.ss.keystore
输入keystore密码: changeit
您的名字与姓氏是什么?
[Unknown]: tns-ssverify.cnnic.cn
您的组织单位名称是什么?
[Unknown]: 中国互联网络信息中心
您的组织名称是什么?
[Unknown]: 中国互联网络信息中心
您所在的城市或区域名称是什么?
[Unknown]: 北京
您所在的州或省份名称是什么?
[Unknown]: 北京
该单位的两字母国家代码是什么
[Unknown]: CN
CN=tns-ssverify.cnnic.cn, OU=中国互联网络信息中心, O=中国互联网络信息中心, L=北京, ST=北京, C=CN 正确吗?
[否]: y
输入<tns-ssverify>的主密码
(如果和 keystore 密码相同, 按回车):
```

图表一创建私钥

请注意: keyEntry\_name 和 keystore\_name 可以根据需要自行输入, 但请与下文中内容保持一致。如果您不指定一个 keystore 名称(不使用参数 -keystore), 则 keystore 文件将保存在您的用户目录中, 文件名为: .keystore。密钥对长度在 -keysize 后面指定, CNNIC 可信网络服务中心要求域名证书密钥对最少为 2048 位。

系统会提示您输入 keystore 密码, 缺省密码为: changeit, 您可以指定一个新的密码, 但请一定要记住。

接着会提示 “What is your first and last name?”, 请输入您要申请域名证书的域名, 而不是真的输入您的个人姓名, 如果您需要为 www.\*\*\*.cn 申请域名证书就不能只输入\*\*\*.cn。域名证书是严格绑定域名的。

接着, 输入您的部门名称、单位名称、所在城市、所在省份和国家缩写(中国填: CN, 其他国家填其缩写), 除国家缩写必须填 CN 外, 其余都可以是英文或中文。这些信息具体内容可以忽略, 生成证书时信息以 RA 系统中登记的为准。



请备份您的 keystore 文件并记下私钥密码。最好是把私钥文件备份到软盘或光盘中。

#### 4) 把CSR发给CNNIC

成功生成 CSR 后请在登录 CNNIC 证书下载页面时把 CSR 内容发给 CNNIC 即可。请一定不要再动您的服务器，等待证书的颁发。

### 3. 下载服务器证书

#### 1) 准备下载证书所需信息

**参考号与授权码：**参考号与授权码是下载证书的密码凭证。当申请的证书通过审核时，用户将接收到由 CNNIC 发送的通过审批的电子邮件通知，该邮件中含有 16 位的参考号与授权码信息，其中参考号与授权码的前 13 位为明文显示，后 3 位为密文显示。审核员会以邮件通知的方式发送后三位的明文显示。

#### 2) 下载证书

登录 CNNIC 可信网络服务中心网页

[http://www.cnnic.cn/jczyfw/wzws/xz/201010/t20101027\\_16322.html](http://www.cnnic.cn/jczyfw/wzws/xz/201010/t20101027_16322.html)

点击页面中部的“可信服务器证书下载”图片链接进入到证书下载页面，如下图所示：

可信服务器证书下载	
<a href="#">点击这里进行在线CSR校验</a>	
参考号：	<input type="text"/>
授权码：	<input type="text"/>
证书请求文件（CSR）：	<p>请把整个CSR文件中 -----BEGIN CERTIFICATE REQUEST----- 和 -----END CERTIFICATE REQUEST----- 之间的内容复制到下边的输入框中</p> <div style="border: 1px solid #ccc; height: 200px; width: 100%;"></div>
<input type="button" value="提交"/> <input type="button" value="重置"/>	

图表四可信服务器证书下载页面

根据网页上的提示输入“参考号”和“授权码”，将证书请求文件中除去头尾“-----BEGINNEWCERTIFICATE REQUEST-----”和“-----ENDNEWCERTIFICATE REQUEST-----”的中间部分内容复制到 CSR 文本框中。结果如下所示：

可信服务器证书下载

[点击这里进行在线CSR校验](#)

参考号：	<input type="text" value="MV4K646JDDHAF6W5"/>
授权码：	<input type="text" value="CJQLNDB7FQSVEJA3"/>
证书请求文件（CSR）：	<p>请把整个CSR文件中 -----BEGIN CERTIFICATE REQUEST----- 和 -----END CERTIFICATE REQUEST----- 之间的内容复制到下边的输入框中</p> <pre style="font-family: monospace; font-size: 0.9em; border: 1px solid #ccc; padding: 5px;"> MIICrDCCA2QCAQAwZzELMAkGA1UEBhMCQ04xEDAOBgNVBAGTB2JlaWppbmcxEDAOBgNVBACTB2JlaWppbmcxDjAMBgNVBAoTBWVudm1jMQ4wDAYDVQLLEwVjbm5pYzEUMBIGA1UEAxMLbTEuY25uaWMuY24wggeiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQCwZKe5sIA8Vv7uYleWQMUVOS7K/dagHhyb9DYKOUOSQqJkHsFzAMUZzyjLkvE2tUTNtMqbPaxV8TGSg+AcC7zNABydQpAUWw91dGoLqGtKdtOsQ/tWdOBb11Oj8amCi/yRxpPSPJPrLisBFCxwt+8wGj8WICj3vP8jOqnpUtkfx3S9AMfaAveGret1UF/80DBboVwJXCTKwcc+dHykjsiswAOiWYlgnArdeXnigR4Ym59IjiFmOfiiBSKbGwVlNXJ21f6DsLFKf8JvZq9Yfdjc135QQPOpzGhR98TKzSTv/6/c+ocG2yexgFtMZac/Z41Jh9iUmNkp69nbs1sHU5FAgMBAAGgADANBgkqhkiG9wOBAAQUFAAOCAQEAqGbSxekMJTPsS7VHuP1YzpkOaxN3D3AAyOoT7MC3pEDnlk49e779Vxr2B13nFbh1                     </pre>

图表五填入收到的参考号和授权码以及生成的 csr

点击“下载”，如果参考号、授权码和 CSR 均无问题，则显示页面如下所示。

### 证书下载-证书生成

证书文件：

```
-----BEGIN CERTIFICATE-----
MIIEGzCCAwwOgAwIBAgIQEMCXznvJBxWzS5X3sUEd6DANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQG
EwJjbjEOMAwGA1UEChMFY25uaWMxEzARBgNVBAMTCmNubmljIHJvb3QwHhcNMTAxMjA3MDkzOTAw
WhcNMTEwMjA3MDkzOTAwWjBhMQswCQYDVQQGEwJDTjENMAAsGA1UECB4EUXdOrDENMAAsGA1UEBx4E
UxdOrDEOMAwGA1UEChMFY25uaWMxEzARBgNVBAsTBWVubmljMRQwEgYDVQQDEwtMS5jbm5pYy5j
bjCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALBkp7mWgDxW/u5iV5ZAxRUSLsr91qAe
HJvONgo645JComQewXMAxRnPKMuS8Ta1RM2Oyps8DFXxMzIb4BwLvMOAHJ1CkBRbD3VOaguo2R2
06xD+1Z3QFuLU6PqxYKL/JHGsk9I8k+suKwEULHC37zAaPxYgKPe8/yM6qe1S2R/HdL0Ax9oC94a
t62VQX/zQMFuhXAlcJMrDBz50fKSoyKzAA6JZiWCCt17GfWBHhibn0iOIWY5+KIFIpsbBUU1cnb
V/ooWsup/wm9mr1h92NyXf1BA86nMaFH3xMrNJO//r9z6hwbbJ7GAW0x1pz9niUmH2JSY2Snr2du
-----
```

Web服务器证书请将证书编码框中的内容拷贝，并粘贴到文本中，保存成Web服务器能够识别的格式。

保存

图表六生成证书

### 注意：关于证书的格式转换

从 CNNIC 获得的证书格式为 X509 格式。该将证书文件的扩展名由 txt 改为 cer 或 crt 后，可在 windows 中双击打开查看证书的相关信息。显示信息类似下图所示：

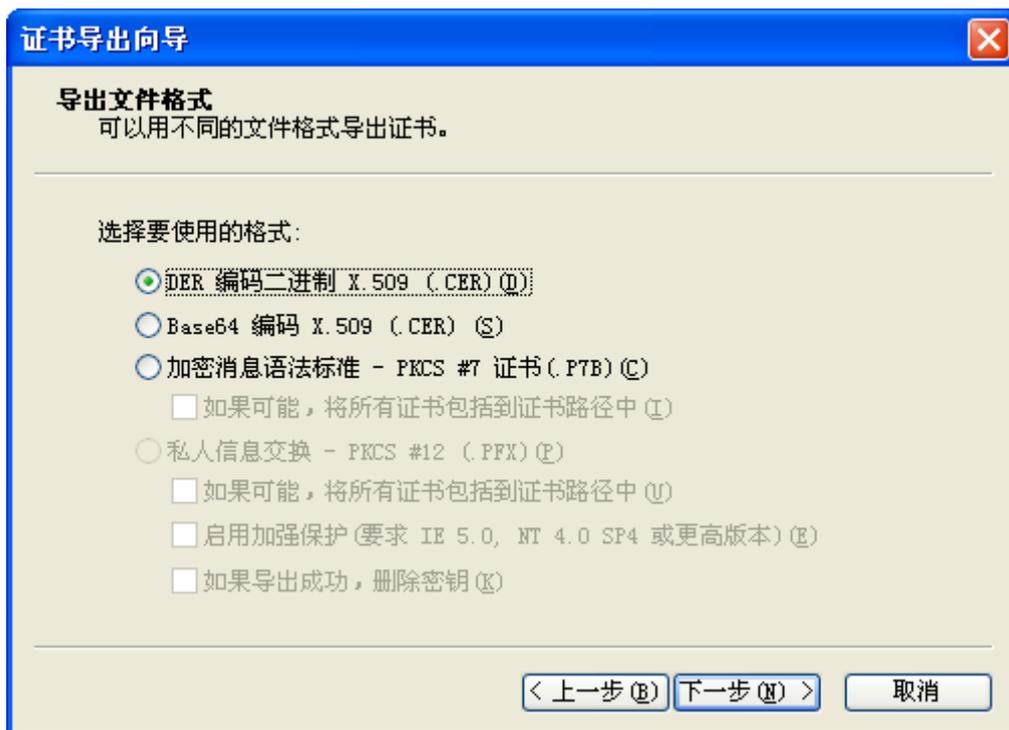


图表七格式转换

X509 格式的证书利用 windows 提供的图形界面操作工具可以另存为以下两种编码格式:

- BASE64 编码格式: 该格式的证书可以用记事本打开
- DER 编码格式: 二进制格式

在上图中, 点击“详细信息”->“复制到文件”后, 即可以根据提示点击“下一步”利用证书导出向导导出需要格式的证书, 如下图所示:



图表八证书导出向导

## 4. 安装根证书和服务证书

### 1) 下载根证书及 CNNIC 中级根证书

下载地址:

快速证书: [http://www.cnnic.cn/jczyfw/wzws/ksym/ksxz/201105/t20110524\\_21055.html](http://www.cnnic.cn/jczyfw/wzws/ksym/ksxz/201105/t20110524_21055.html)

标准证书: [http://www.cnnic.cn/jczyfw/wzws/bzcx/xz/201010/t20101027\\_16322.html](http://www.cnnic.cn/jczyfw/wzws/bzcx/xz/201010/t20101027_16322.html)

EV证书: <http://www.cnnic.cn/jczyfw/wzws/kxEV/xz/>

将 CNNIC 中级根证书文件名保存为“CNNIC.cer”，将根证书文件名保存为“root.cer”

### 2) 将根证书 root.cer 导入到 Keystore 文件

命令格式: `keytool -import -trustcacerts -aliasroot -fileroot.cer -keystore [keystore_name]`

注: []中的内容为需要输入的参数, 以上命令间都有空格

- `keystore_name`: 表示保存证书私钥的文件名, 扩展名一般为 `keystore`

```
C:\Users\micah\Desktop\key>keytool -import -trustcacerts -alias root -file CNNIC
ROOT.cer -keystore tns-ssverify.keystore
输入keystore密码:
Owner: CN=CNNIC ROOT, O=CNNIC, C=CN
发照者: CN=CNNIC ROOT, O=CNNIC, C=CN
序号: 49330001
有效期间: Mon Apr 16 15:09:14 CST 2007 至: Fri Apr 16 15:09:14 CST 2027
认证指纹:
MD5: 21:BC:82:AB:49:C4:13:3B:4B:B2:2B:5C:6B:90:9C:19
SHA1: 8B:AF:4C:9B:1D:F0:2A:92:F7:DA:12:8E:B9:1B:AC:F4:98:60:4B:6F
信任这个认证? [否]: y
认证已添加至keystore中
```

此 keystore 为之前生成的那个。

图表九导入根证书

### 3) 将中级CA证书CNNIC.cer导入keystore文件

命令格式: `keytool -import -v -trustcacerts -storepass [password] -alias`

`[ca_cert] -file CNNIC.cer -keystore [keystore_name]`

注: []中的内容为需要输入的参数, 以上命令间都有空格

- `password`: 表示私钥的保护口令
- `ca_cert`: 表示中级 CA 证书文件名
- `keystore_name`: 表示保存证书私钥的文件名, 扩展名一般为 `keystore`

```
C:\Users\micah\Desktop\key>keytool -import -trustcacerts -alias INTER -file CNNI
C.cer -keystore tns-ssverify.keystore
输入keystore密码:
认证已添加至keystore中
```

图表十导入中级根证书

此 keystore 为之前生成的那个。

### 4) 将服务器证书ml.cnnic.cn.cer导入到keystore文件

命令格式: `keytool -import -v -trustcacerts -storepass [password] -alias`

**[alias\_name] -file [keyEntry\_name] -keystore [keystore\_name]**

注：[]中的内容为需要输入的参数，以上命令间都有空格

- password: 表示私钥的保护口令
- server\_cert: 表示服务器证书文件名
- keyEntry\_name:表示私钥的别名
- keystore\_name: 表示保存证书私钥的文件名，扩展名一般为 keystore

```
C:\Users\micah\Desktop\key>keytool -import -trustcacerts -alias tns-ssverify -file tns-ssverify.der.cer -keystore tns-ssverify.keystore
输入 keystore 密码:
认证回复已安装在 keystore 中
```

图表十一导入服务器证书

此 keystore 为之前生成的那个。

请注意：如果您在生成 keystore 没有指定名称，则不需要-keystore 选项。

在运行此命令时会提示您输入密码，也就是您在生成 keystore 时设置的密码。

当导入证书到您的 keystore 时，一定要使用生成 CSR 时一样的别名(alias)，同时使用-trustcacerts 参数。如果不指定一样的别名，将不能安装成功！

## 5) 查看keystore证书

命令格式：**keytool -list -keystore [keystore\_name]**

注：[]中的内容为需要输入的参数，以上命令间都有空格

- keystore\_name: 表示保存证书私钥的文件名，扩展名一般为 keystore

```
E:\resin\resin-2.1.17>keytool -list -keystore m1.cnnic.cn.keystore
输入keystore密码:
Keystore 类型: JKS
Keystore 提供者: SUN

您的 keystore 包含 3 输入

cnnic, 2010-12-9, trustedCertEntry,
认证指纹 (MD5): 27:63:91:3F:CC:40:A4:54:33:EE:F6:BC:91:25:A7:86
m1.cnnic.cn, 2010-12-9, PrivateKeyEntry,
认证指纹 (MD5): 61:6F:74:C3:2A:1D:14:88:72:D2:07:47:50:F3:75:75
roottest, 2010-12-9, trustedCertEntry,
认证指纹 (MD5): 12:3F:2F:19:D3:0F:35:6A:55:C4:68:63:55:D8:72:7E

E:\resin\resin-2.1.17>
```

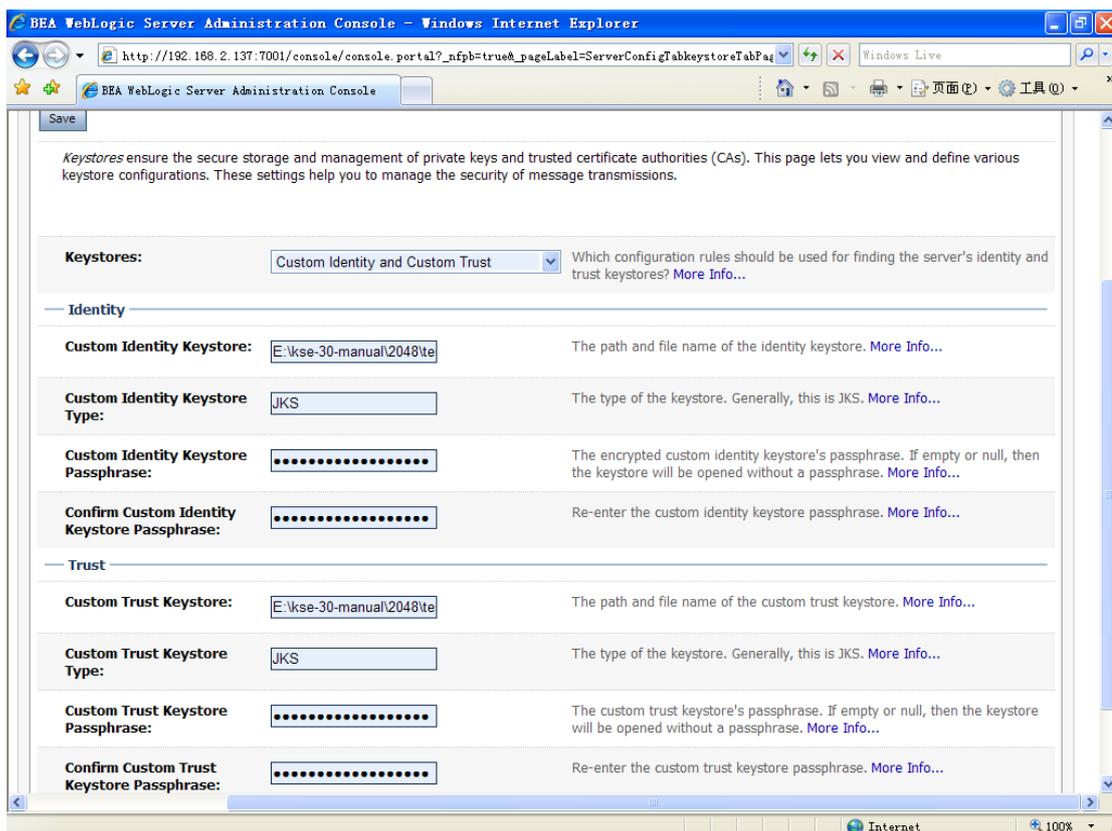
图表十二查看 keystore 证书

## 5. 配置 Weblogic

（下述 Weblogic 配置示例使用的是 Windows 系统下的 weblogicserver9.2，各版本可能会有所不同，请查看 Weblogic 帮助手册中 SSL 部分或咨询 Weblogic 服务提供商）

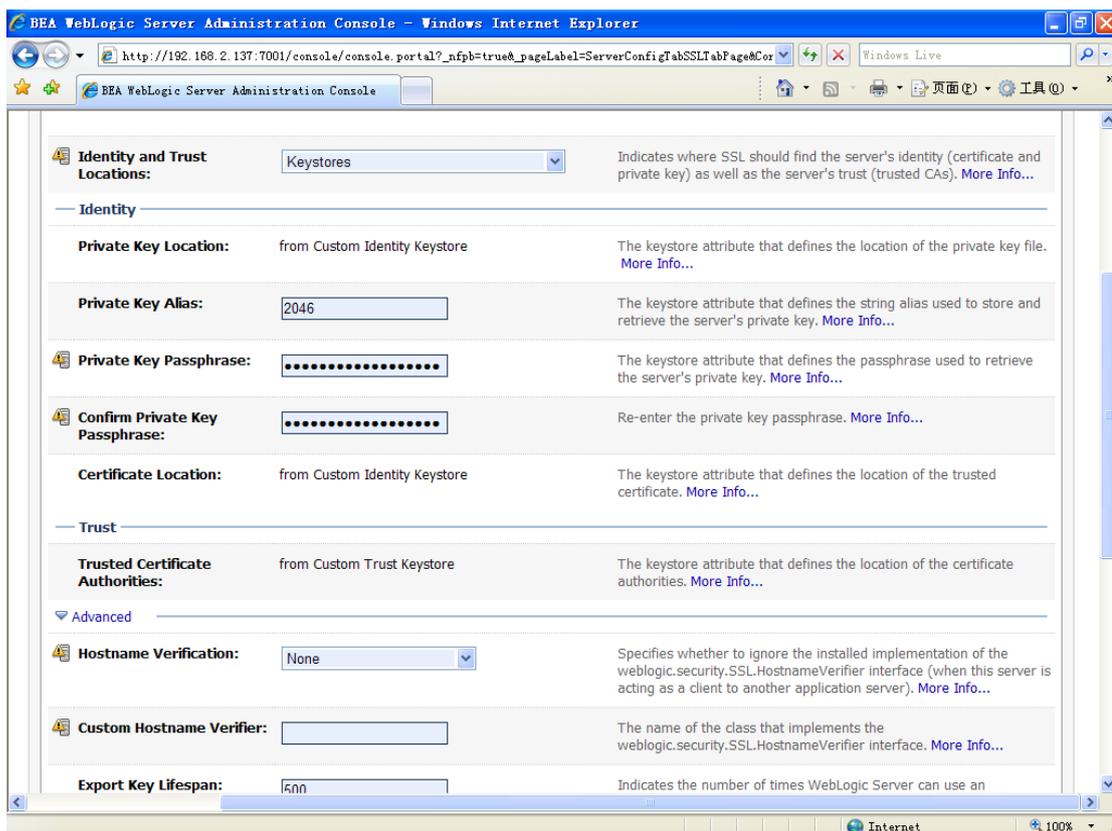
访问 <http://hostname:port/console>，输入用户名和密码（默认都是weblogic）然后登录控制台页面，选中左边菜单中“Environment”→“Server”→选中列表中的服务，点击打开。

打开后在右边列表中选择“keystores”，如图：



图表十三修改配置一

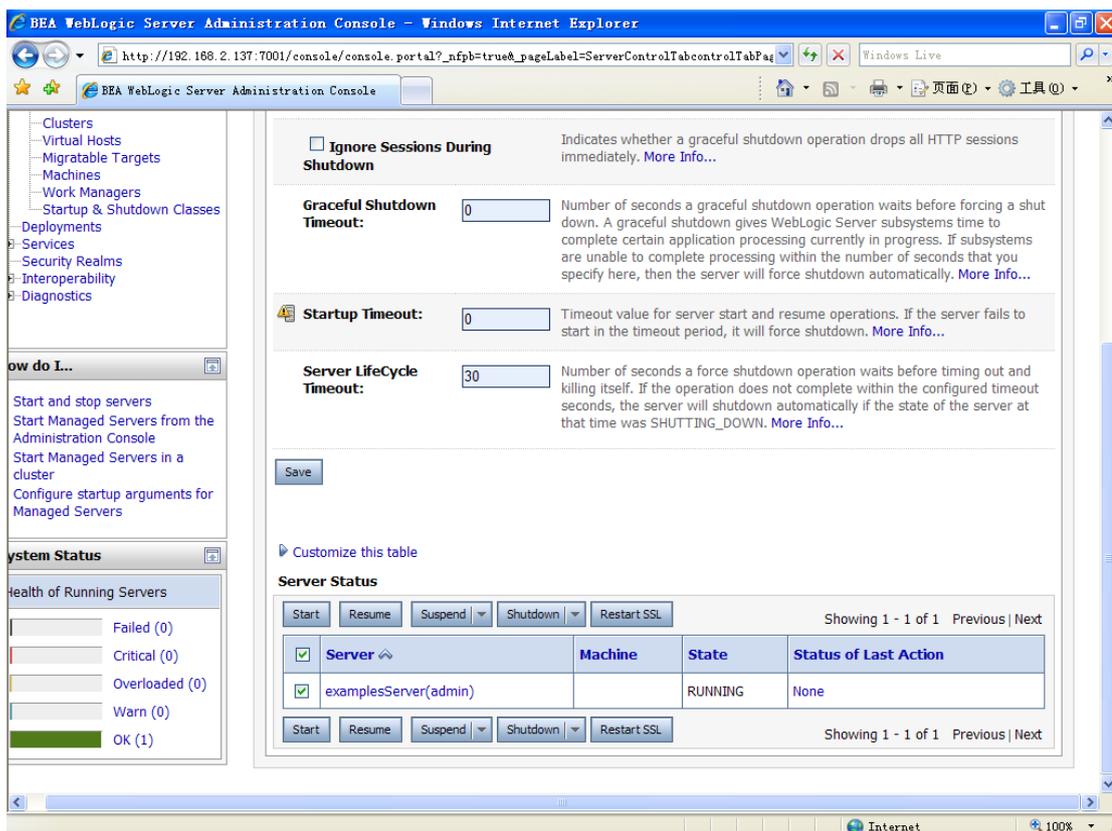
根据实际情况设置证书和 CA 根证书。确认修改的配置，然后保存。  
配置完成“keystore”后，配置右边的 SSL：



图表十四修改配置二

根据实际情况设置。

设置完毕后保存，然后点击“control”，点击“RestartSSL”

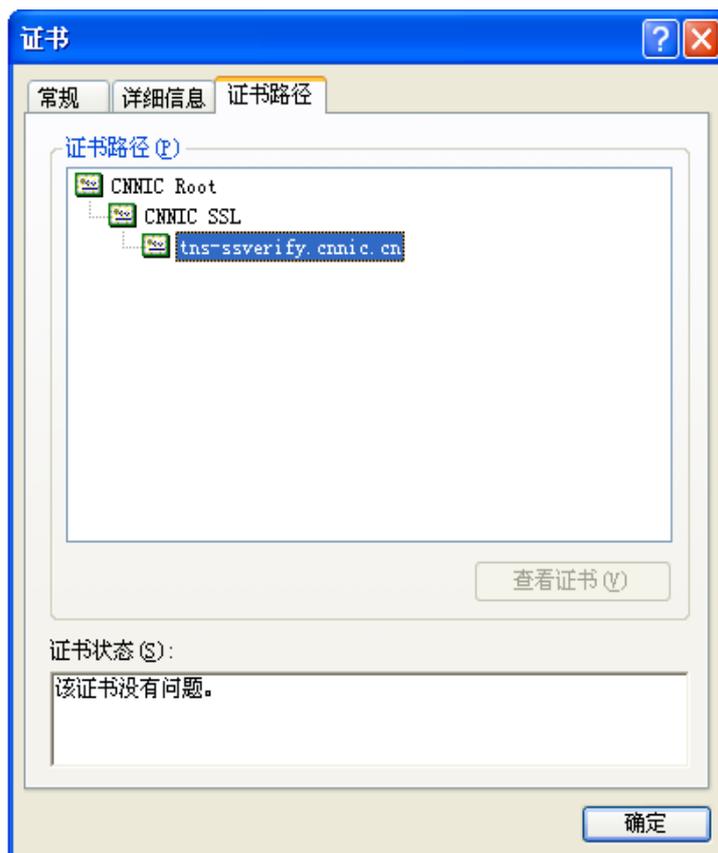


图表十五修改配置三

重启 SSL 服务。然后保存并激活配置。

## 6. 完成配置

如果分配了 7002 端口给 https 服务，且域名解析正确。则在浏览器地址栏输入：<https://tns-ssverify.cnnic.cn>: 7002 (申请证书的域名) 测试您的域名证书是否安装成功，如果成功，则浏览器下方会显示一个安全锁标志。其中证书路径中可以看到根证书显示为 CNNICRoot。



图表十六安装成功后显示服务器证书

请注意：如果您的网页中有不安全的元素，则会提供“是否显示不安全的内容”，建议修改网页删除不安全的内容。

配置成功后，可以根据自己的需要调整 https 所使用的端口，https 访问使用的默认端口是 443。