



**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 10 & 11 版本**

修订日期：2017/05/25

## 目 录

目 录.....	1
一、 部署前特别说明.....	2
二、 合成 JKS 证书.....	2
1. 获取证书.....	2
2. 私钥证书.....	3
3. 合成证书.....	3
三、 安装服务器证书.....	4
1. 配置服务器 SSL 证书.....	4
1) 配置认证模式.....	6
2) 配置服务器证书私钥别名.....	6
3) https 访问测试.....	8
四、 备份和恢复.....	8
1. 备份服务器证书.....	8
2. 恢复服务器证书.....	8
五、 证书遗失处理.....	8



## 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;




## 二、合成 JKS 证书

### 1. 获取证书

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



上根证书 GDCA\_TrustAUTH\_R5\_ROOT.cer 和相应的 CA 证书。如果您申请的是 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 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*）


名称	修改日期	类型
 GDCA TrustAUTH R4 EV SSL_CA.cer ← 中级证书	2017/5/3 9:50	安全证书
 GDCA TrustAUTH R5 ROOT.cer ← 顶级证书	2017/5/3 9:50	安全证书
 testweb.95105813.cn.cer ← 公钥证书	2017/5/3 10:52	安全证书

Globalsign 产品获得证书如下图：

名称	修改日期	类型	大小
 证书文件.crt	2017/5/24 14:37	安全证书	3 KB
 中级根.crt	2017/5/24 14:37	安全证书	2 KB

## 2. 私钥证书

申请证书提交 csr 时会生成一个.key 文件，该文件为证书的私钥，后面配置要用到。

名称	修改日期	类型	大小
 testweb.95105813.cn.csr	2017/5/24 14:37	CSR 文件	3 KB
 testweb.95105813.cn.key ← 证书私钥	2017/5/24 14:37	KEY 文件	2 KB

## 3. 合成证书

- 1)用浏览器打开以下链接: [https://www.trustauth.cn/SSLTool/tool/export\\_keystore.jsp](https://www.trustauth.cn/SSLTool/tool/export_keystore.jsp)
- 2) 用记事本或者文本编辑器打开上面的证书公钥、证书私钥、中级证书文件，根据下图填入合成证书信息，导出后会下载一个 www.domainname.com.jks 的文件，保存好这个文件。



数安时代 | SSL免费工具

### 在线导出Keystore

**CRT证书**

```
nLbJnmDPiJSAIxxUu7TTpuonITQvHqahWVbkBcOwdbSf486NoreyShEG2i5pkPr  
jWnsjyngVZFyNzle/UNIKkxKl2lz9sVYtACrdilYdfhFI5p0pveOviDM+mu9fm17  
kSVv4prcqaq+5iq/ud1gg14V5ZUcFsxBDsgWD643KL1N9X63OvindVBlvp40sptx  
IMAG  
-----END CERTIFICATE-----
```

← 证书公钥

**私钥 Private Key**

```
34iUIMqnFYBBsaf8qPCDntO9C9BDaddLHlnupVQY/XwNwukmf+Et5Rbe4XslWBI4Xdp6YkutUBKq  
8jahAoGAJU6IXpVGEHEuK9MOnKP7N2HTzYtqQOFClJDhc6WqDjkw/Daw6P5B37Z7TelrnGzv5FM  
Z0My2PeAkKarsrswpPNA5oHDQCvQvVnsRoCmUHB5Zt826EtpHy/zD50GwsSghi060hi6ki0ef  
Ve+dHx7ypNgNVmd+ZBIW/q+M+/E=  
-----END PRIVATE KEY-----
```

← 证书私钥.key，在生成csr的时候已经生成

**CA 根证书**

```
nLbJnmDPiJSAIxxUu7TTpuonITQvHqahWVbkBcOwdbSf486NoreyShEG2i5pkPr  
jWnsjyngVZFyNzle/UNIKkxKl2lz9sVYtACrdilYdfhFI5p0pveOviDM+mu9fm17  
kSVv4prcqaq+5iq/ud1gg14V5ZUcFsxBDsgWD643KL1N9X63OvindVBlvp40sptx  
IMAG  
-----END CERTIFICATE-----
```

← 中级证书

**Keystore密码**

..... ← 设置密码，请牢记！

导出KeyStore格式

在线客服：95105813 粤ICP备05036352号 公安备案：4406053010643

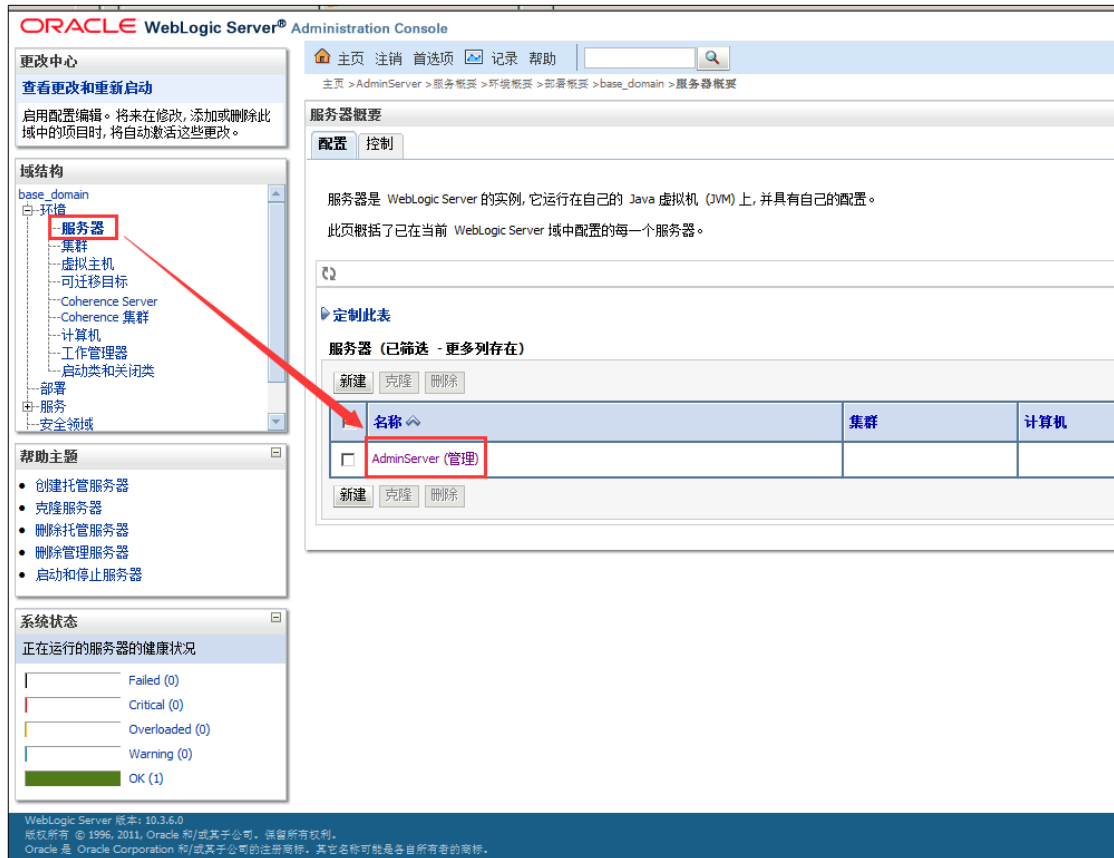
- 在线生成CSR
- 在线解码CSR
- 在线解码CRT证书
- 证书和私钥匹配检测
- 在线导出PFX、PKCS12
- 在线导出Keystore**

## 三、安装服务器证书

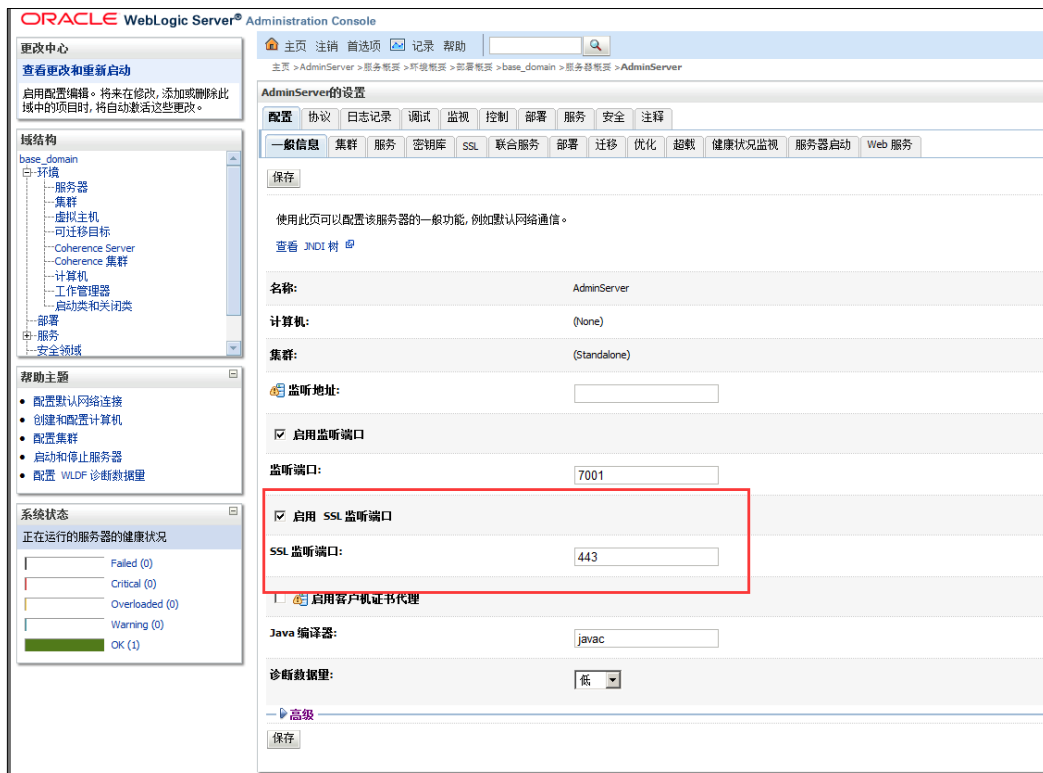
### 1. 配置服务器 SSL 证书

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, 修改为 ssl 默认监听端口 443, 或者根据实际情况修改 ssl 端口号：



## 1) 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：



## 2) 配置服务器证书私钥别名

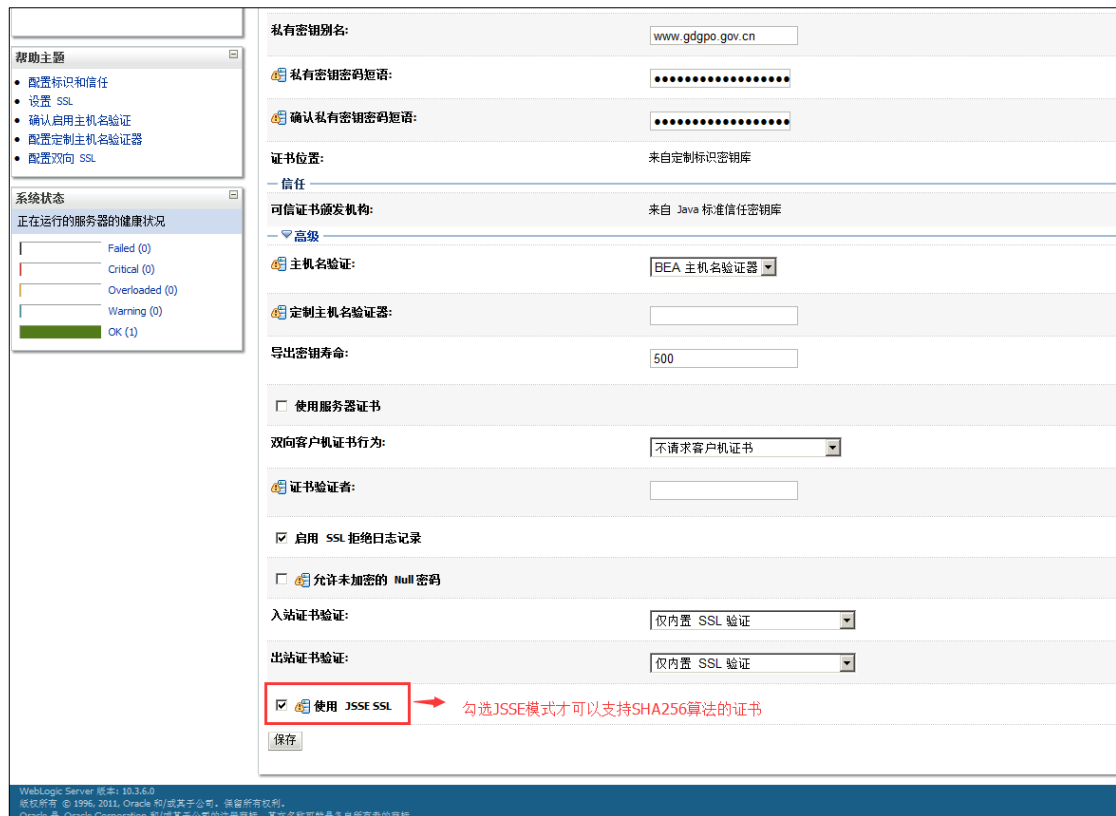
在“SSL”下需要配置密钥库中的私钥别名信息。私钥别名和证书的域名相同，通常设置的私钥保护密码和 keystore 文件保护密码相同。

输入私钥别名“www.domain.comn”，并输入私钥密码。





点击高级，勾选使用“JSSE SSL”







### 3) 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。

## 四、 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

备份好步骤一生成的 [www.domainname.com.jks](http://www.domainname.com.jks) 文件,并且牢记密码。

### 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。

## 五、 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。

