Weblogic 10.3.6

二〇二一年一月

GlobalSign
GMO INTERNET GROUP

目 录

服务器证书安装配置指南（Weblogic 10.3.6）

1. 生成证书请求

1.1 安装JDK（可选）

Weblogic 安装后自带JDK 安装。如果您直接在服务器上生成证书请求，请进入Weblogic安装目录下JDK 所在路径的bin 目录，运行keytool 命令。

如果您需要在其他环境下生成证书请求文件，则您可以选择安装JDK，稍后上传生成的密钥库文件keystore.jks 到服务器上进行配置。

可以参考Java SE Development Kit (JDK) 下载。下载地址：

http://java.sun.com/javase/downloads/index.jsp

1.2 生成keystore 文件

生成密钥库文件keystore.jks 需要使用JDK 的keytool 工具。命令行进入JDK 下的bin目录，运行keytool 命令。（示例中粗体部分为可自定义部分，请根据实际配置情况作相应调整）

keytool -genkey -alias **server** -keyalg RSA -keysize 2048 -keystore **keystore.jks** -storepass **password**

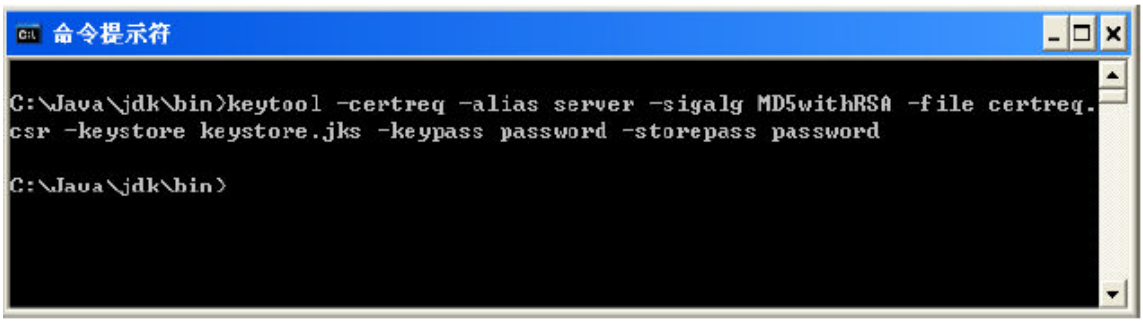
```
CN=cn.globalsign.com, OU=IT Dept, O= GlobalSign China Co., Ltd., L=Shanghai, ST=Shanghai, C=CN
正确吗?
  [否]:  Y
```

```
输入<weblogic>的主密码
        （如果和 keystore 密码相同，按回车）:
```

以上命令中，server 为私钥别名(alias)，生成的keystore.jks 文件默认放在命令行当前路径下。

1.3 生成证书请求文件(CSR)

keytool -certreq -alias **server** -sigalg MD5withRSA -file **certreq.csr** -keystore **keystore.jks** -keypass **password** -storepass **password**



请将证书请求文件certreq.csr 提交给GlobalSign，并备份保存证书密钥库文件keystore.jks，等待证书的签发。密钥库文件丢失将导致证书不可用。

2. 导入服务器证书

2.1 获取中级CA 证书

为保障服务器证书在 IE7 以下客户端的兼容性，服务器证书需要安装两张中级 CA 证书（包括中级证书和交叉证书）。

从邮件中获取中级证书和交叉证书：

将证书签发邮件中的从 BEGIN 到 END 结束的两张中级 CA 证书内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）分别粘贴到记事本等文本编辑器中，并修改文

件扩展名，保存为 intermediate1.cer (交叉证书)和 intermediate2.cer (中级证书)文件。

2.2 获取服务器证书

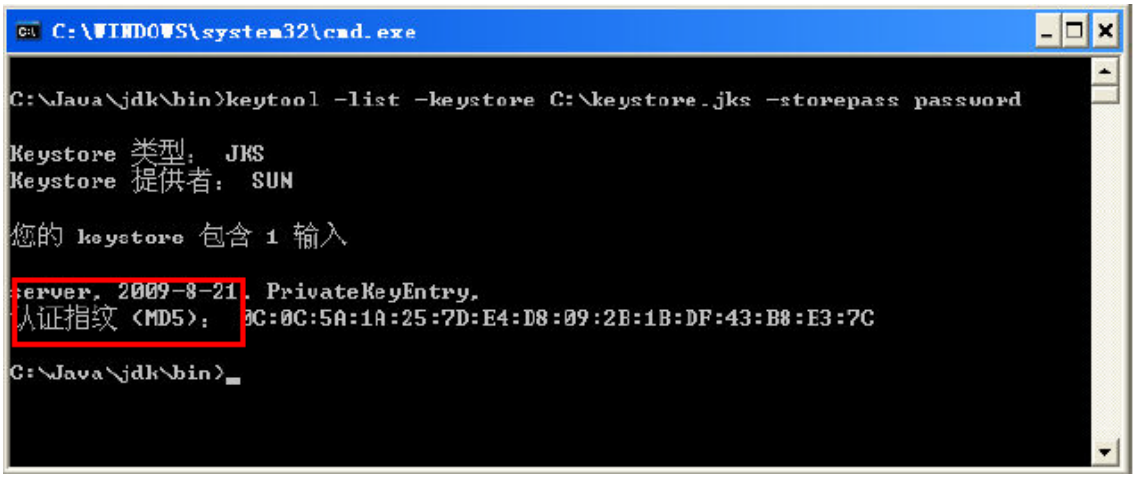
将证书签发邮件中的从 BEGIN 到 END 结束的服务器证书内容（包括”-----BEGIN CERTIFICATE-----"和”-----END ERTIFICATE-----” ）粘贴到记事本等文本编辑器中，并修改文件扩展名保存为server.cer文件。

查看Keystore文件内容

进入 JDK 安装目录下的 bin 目录，运行 keytool 命令。

您的keystore 密码

keytool -list -keystore **C:\keystore.jks** -storepass **password**



查询到 PrivateKeyEntry 属性的私钥别名(alias)为server。记住该别名，在稍后导入服务器证书时需要用到。（示例中粗体部分为可自定义部分，请根据实际配置情况作相应调整。）

注意，导入证书时，一定要使用生成证书请求文件时生成的 keystore.jks 文件。keystore.jks 文件丢失或生成新的 keystore.jks 文件，都将无法正确导入您的服务器证书。

2.3 导入证书

导入第一张中级 CA 证书（交叉证书）

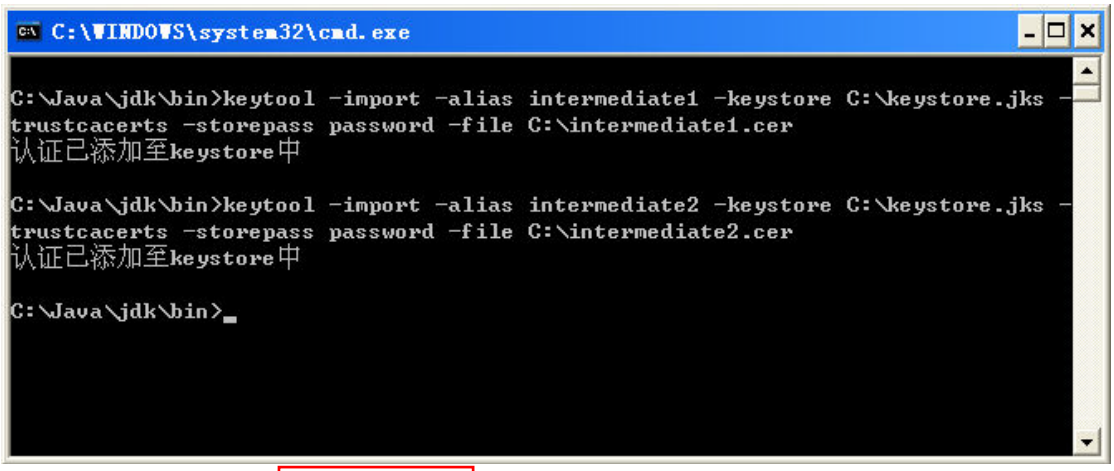
keytool -import -alias **intermediate1** -keystore **C:\keystore.jks** -trustcacerts -storepass

password -file **C:\intermediate1.cer**

导入第二张中级 CA 证书（中级证书）

keytool -import -alias **intermediate2** -keystore **C:\keystore.jks** -trustcacerts -storepass

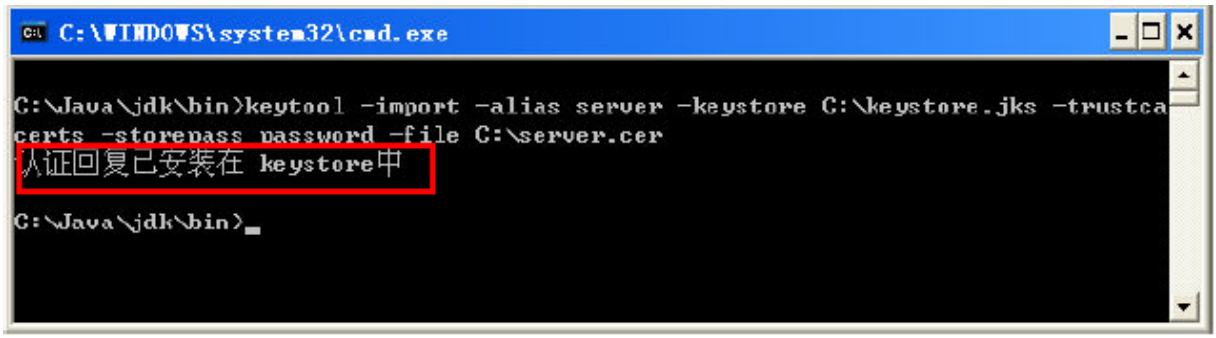
password -file **C:\intermediate2.cer**



导入服务器证书　　私钥的别名

keytool -import -alias **server** -keystore **C:\keystore.jks** -trustcacerts -storepass

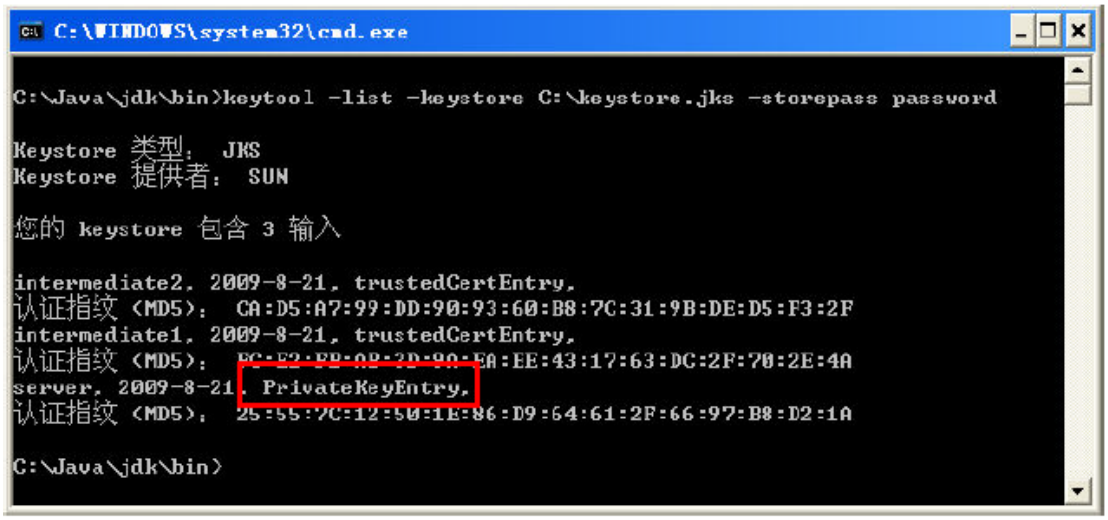
password -file **C:\server.cer**



导入服务器证书时，服务器证书的别名必须和私钥别名一致。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”。证书导入完成，运行keystool 命令，

再次查看keystore 文件内容

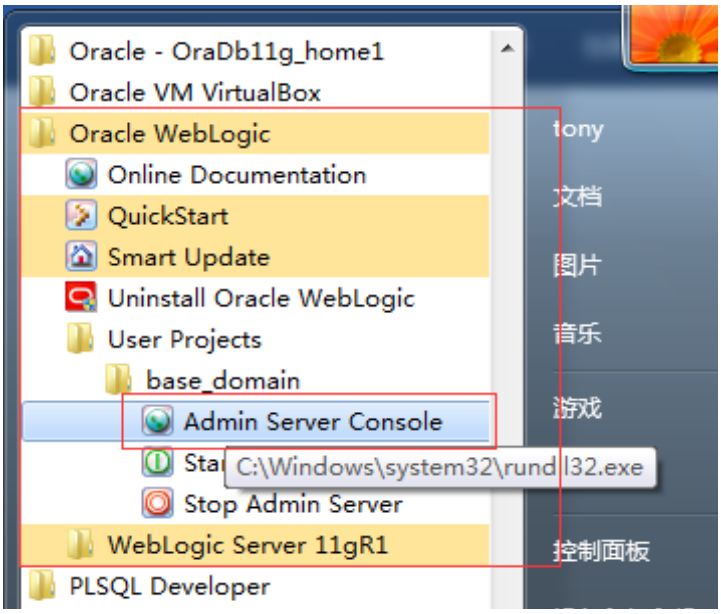
keytool -list -keystore **C:\keystore.jks** -storepass **password**



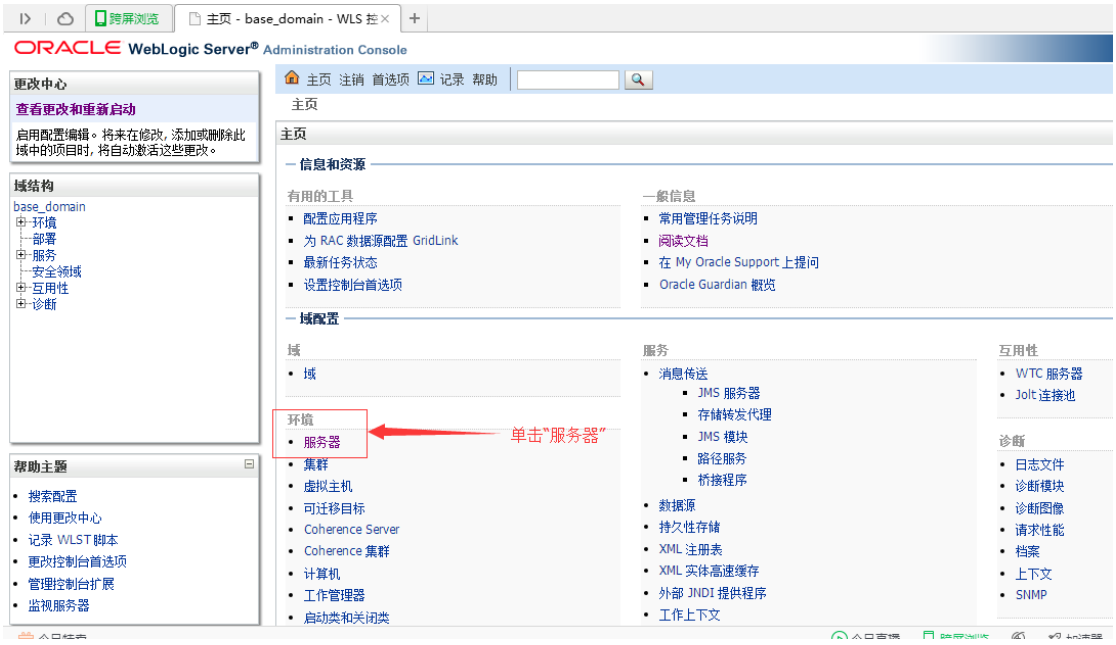
3. 安装服务器证书

3.1 配置Servers

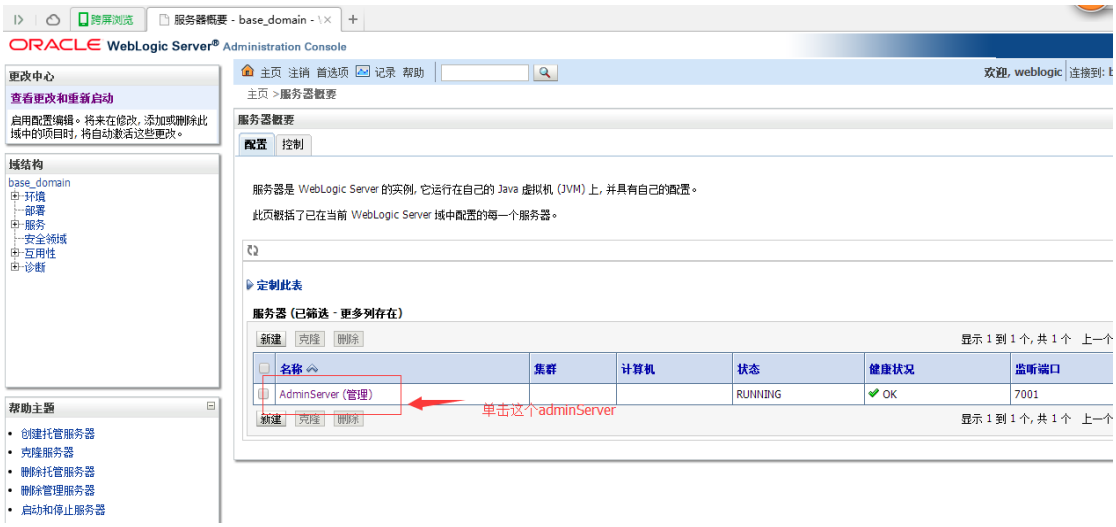
登陆Weblogic 控制台



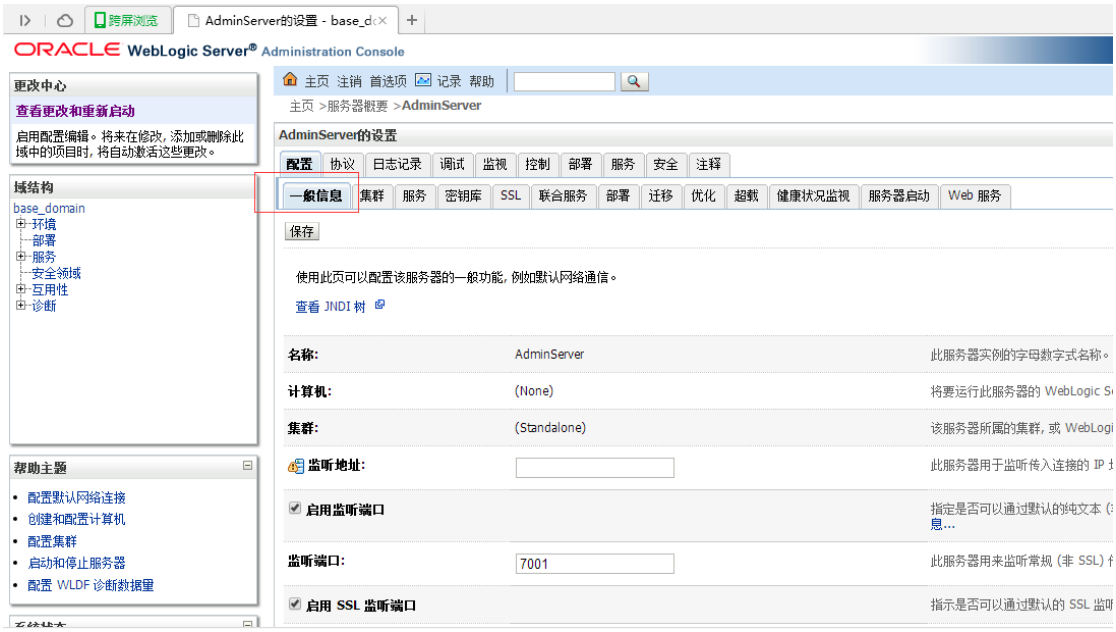
2.单击“服务器”，并进入“服务器”

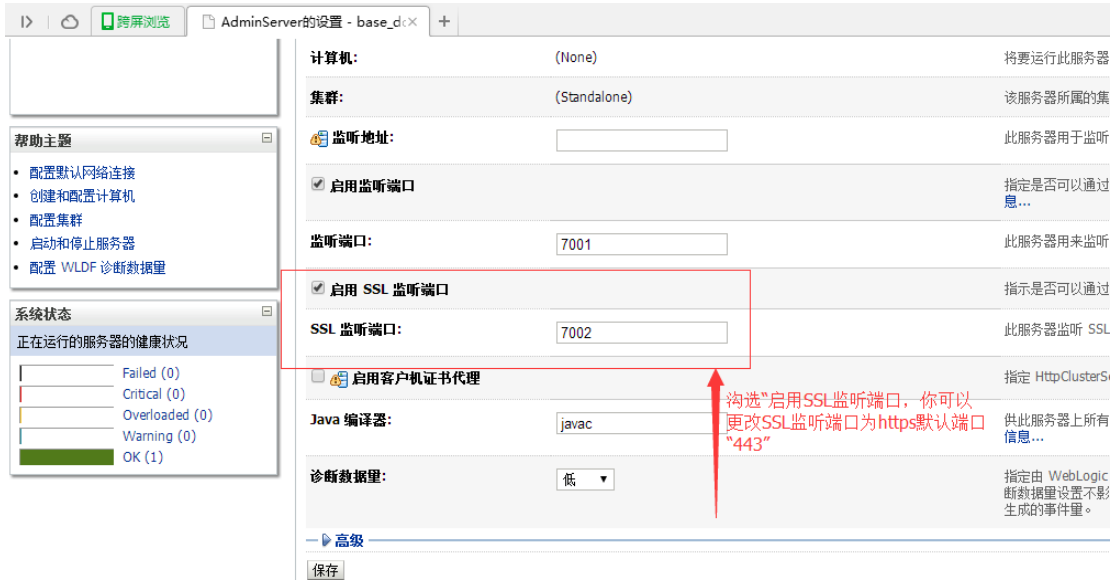


3.选择您需要配置服务器证书的服务器（server）



4.在“一般信息（General）”下，可以配置您的 https 是否启用，以及访问的端口号。Weblogic SSL 默认端口是 7002，你可改更成 https 默认端口号为 443，以方便访问 https 不用输入端口，请勾选“启用 SSL 监听端口”并修改端口号。



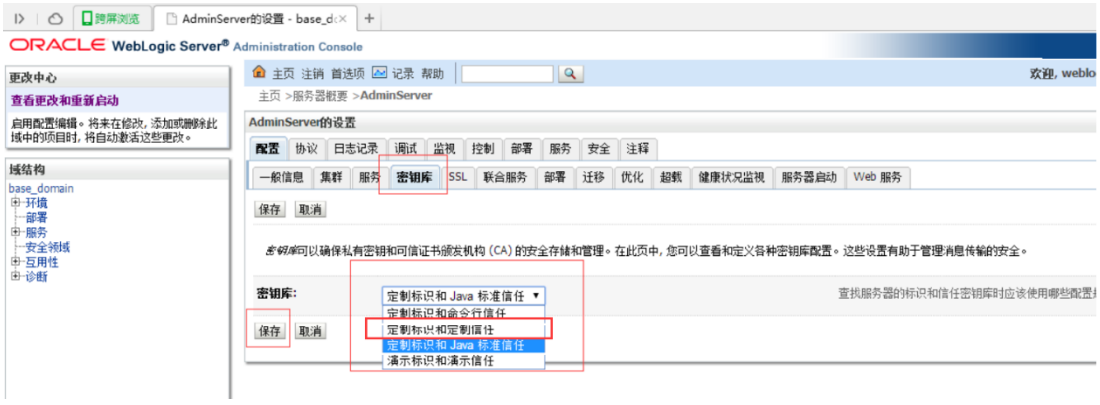


3.2 设置认证模式

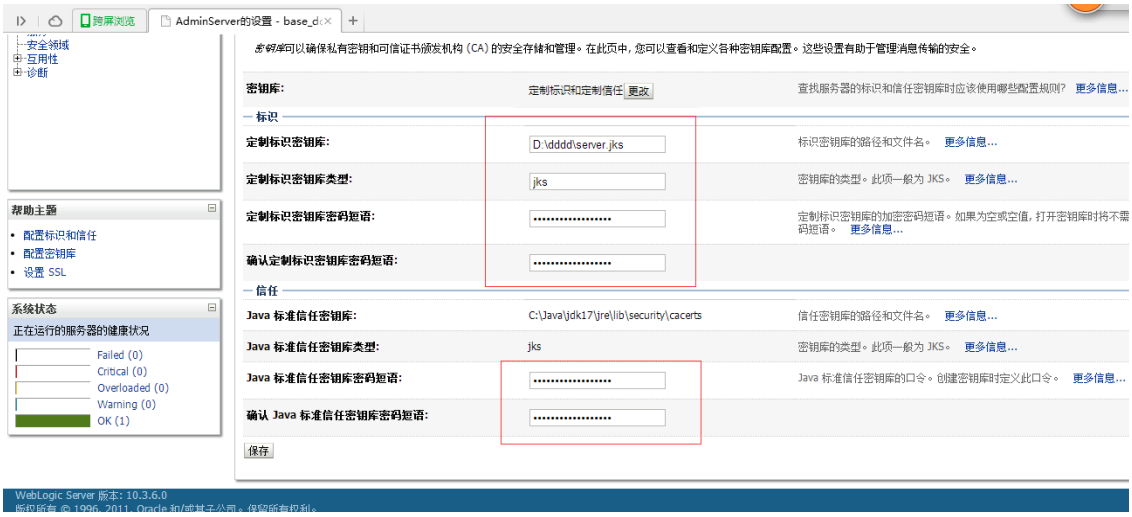
选择“Keystores”，并配置认证方式

服务器单向认证选择“定制标识和 JAVA 标准信任”(Custom identity and Java Standard Trust)，

双向认证选择“定制标识和定制信任”（Custom Identity and Custom Trust）



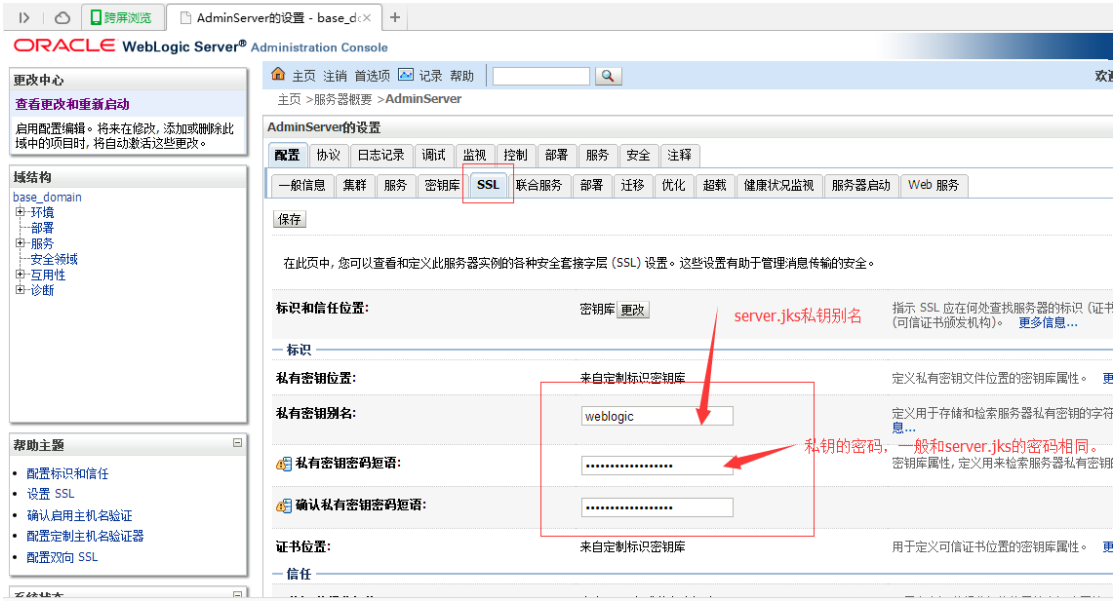
将您的密钥库文件 keystore.jks 保存到服务器上相应目录，并配置其路径和密钥库文件保护密码。



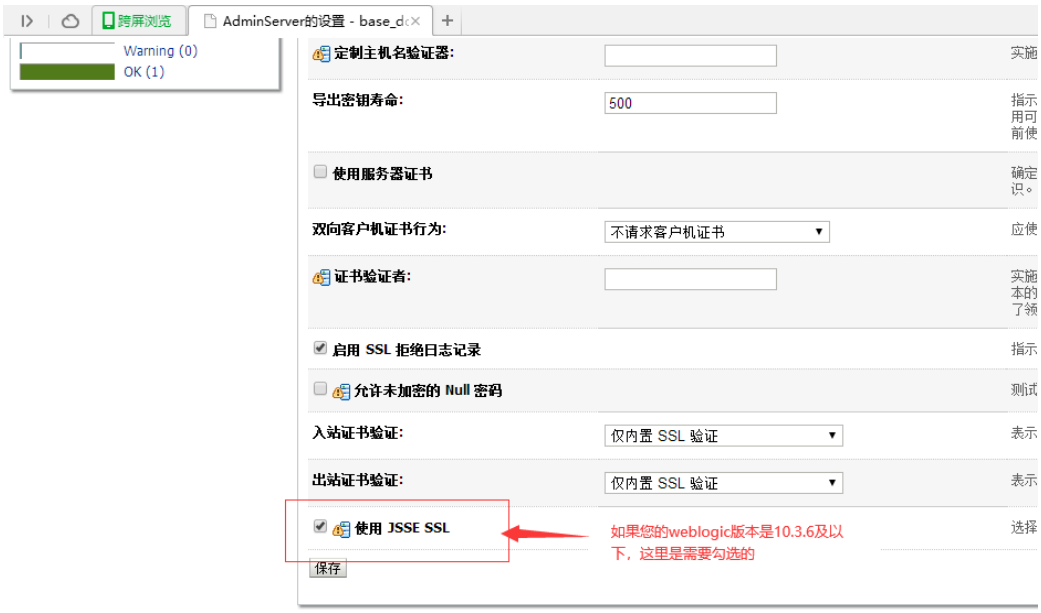
单向认证中，需要配置 JRE 默认信任库文件 cacerts。cacerts 默认密码为 changeit。

3.3 设置服务器证书私钥别名

在“SSL”下配置密钥库中的私钥别名信息。私钥别名可以使用 keytool –v -list –keystore server.jks 命令查看。通常私钥保护密码和 keystore(server.jks)文件保护密码相同。



weblogic 12c 版本及以上是完美支持 sha256 的证书， 但是要是 weblogic 11g(10.3.6)及以下版本，需要在 ssl 设置里的高级选项中勾选“使用 JSSE SSL”，才可以支持 sha256 证书。



设置完成后，保存所有修改。如果系统提示需要重启 Weblogic，则您需要重启后才能使配置生效。

3.4 访问测试

在每一步设置过程中请注意随时保存所做的修改，完成所有配置后，就可以立即通过您设定的SSL 端口号，访问https://youdomain:port 测试证书的安装情况了。

4. 服务器证书的备份及恢复

在您成功的安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您带来不便。

4.1 服务器证书的备份

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。

4.2 服务器证书的恢复

请参照服务器证书安装部分，将服务器证书密钥库 keystore.jks 文件恢复到您的服务器上，并修改配置，恢复服务器证书的应用。

请注意，此文档会不定期更新！

GlobalSign China Co., Ltd

环玺信息科技（上海）有限公司

2021年 1 月