

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

修订日期: 2017/05/25



目录

-,	部署前特别说明	2
-,	合成 JKS 证书	3
1.	获取证书	3
2.	私钥证书	3
3.	合成证书	4
二、	安装服务器证书	4
1.	配置 WEBLOGIC 服务器证书	4
2.	配置认证模式	6
3.	配置服务器证书私钥别名	7
4.	нттрs 访问测试	8
三、	备份和恢复	8
1.	备份服务器证书	8
2.	恢复服务器证书	9
四、	证书遗失处理	9



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;





一、 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*)

0 安全证书
0 安全证书
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

请找到之前提交 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	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: <u>https://www.trustauth.cn/SSLTool/tool/export_keystore.jsp</u>

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.domainame.com.jks 的文件,保存好这个文件。

线导出Keystore	
CRT证书	在线生成CSR
I b InmDPil ISAlyy I uZTTnuonTOvHrahW//bkBcOwdbSf/86NoreySbEC2/5nkPr	▲在线解码CSR
WnsjyngVZFyNzle/UNIKkxKi2lz9sVYtACrdiLydfhFl5p0pyeOvIDM+mu9fm17	在线解码CRT证书
KSVV4prcqae+5ig/uq1qg14V52UcFsXBDSGWD643KL1N9X63UVindVBIVp4UsptX 证书公钥 IMAG END CERTIFICATE	▼ 证书和私钥匹配检测
私钥 Private Key	在线导出PFX、PKCS12
34JUJMgnFYBBsaf8gPCDNt09C9BDaddLHInupV0Y/XwNwukmf+Ft5Rbe4XsIWBj4Xdp6YkutUBKg BjahAoGAJU6IXpVGEHEuK9MOnKP7N2HTzYtgQOFCJJDhc6WgDJkwx/Daw6P5B37Z7TeIrnGzv5FM Z0My2PeAkKarsrswypPNIA5oHDQCv0QvVnsRoCmUHB5Zt826Etphy/zD50GwsSghl060hl6kl0ef Ve+dHx7ypNgNVmd+7BjW/q+M+/E= END PRIVATE KEY	▲ 在线导出Keystore
CA 根证书	
nLbJnmDPiIJSAlxxUu7TTpuonITQvHqahWVbkBcOwdbSf486NoreyShEG2i5pkPr IWnsjvngVZFvNzle/UNIKkxKi2Iz9sVYtACrdiLvdfhFI5p0pveOvIDM+mu9fm17 kSVv4prcqae+5ig/ud1qa14V5ZUcFsxBDSGWD643KL1N9X63OvindVBlvp40sptx IMAG END CERTIFICATE	
Keystore密码	

二、 安装服务器证书

1. 配置 Weblogic 服务器证书

登陆 Weblogic 控制台,点击-环境-服务器:





WebLogic Server	官理控制合 12C							
更改中心	▲ 主页 注销 首选项 🗠 记录 帮助	Q						
查看更改和重新启动	王贞							
启用配置编辑。将来在修改,添加或删除此	主页							
域中的项目时,将自动激活这些更改。	一信息和资源							
域结构	有用的工具	一般信息						
Dase_domain 中·环境 一·部署 一·册略务 一·安全领域 中·互用性 由·诊断	 配置应用程序 为 RAC 数据源配置 GridLink 配置动态集群 最新任务状态 设置控制台首选项 一 域配置 域	 常用管理任务说明 阅读文档 在 My Oracle Support 服务 消息传送 JMS 服务器 						
帮助主题 E 搜索配置 使用更改中心 记录 WLST 脚本 更改控制台首选项 管理控制台首选项	 环境 ・服务器 ・果群 ・服务器模板 ・可迁移目标 ・Coherence 集群 ・计算机 ・虚拟主机 	 JMS 服务器 存储转发代码 JMS 模块 路径服务 桥接程序 数据源 持久性存储 XML 注册表 XML 实体高速缓存 						

在服务器列表里选择要配置 SSL 证书的服务器

	理控制台	12c									
更改中心 金 主页 注請 首选项 回 注 記示 即な 思助 Q											
查看更改和重新启动 主页 > 服务器概要											
启用配置编辑。将来在修改,添加或删除此	服务器概要										
1%中的项目时,将自动激活这些更改。	配置 控制										
域结构											
base_doman 中 环境 一 邮署 中 服务 一 安全领域 中 互用性 田 诊断	服务器是 WebLogic Server 的实例, 它运行在自己的 Java 虚拟机 (JVM)上, 并具有自己的配置。 此页版括了已在当前 WebLogic Server 域中配置的每一个服务器。										
	服务器 (已筛选 - 更多列存在)										
	新建 克隆 刪除										
		名称 🗇	类型	集群	计算机	状态	儲				
		AdminServer (管理)	已配置			RUNNING	4				
帮助主题 🛛	新	建 克隆 删除									
 创建托管服务器 克隆服务器 											

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为 443:





西北山 2] 命 主而注	销 首诜师 🔼	1 记录 表	sati I T			0								
更成甲心	→ 主火 注 主页 > 服务	·器概要 >Adn	inServe	r											
自有更以相望制后约 自田町罢编辑。这本在修改 法加苏明除此	AdminServe	AdminServer的设置													
域中的项目时,将自动激活这些更改。	配置 协议	· 控制 · 部署 · 服务 · 安全 · 注释													
域结构	一般信息	集群 服务	联合	調査	部署	迁移	优化	超载	健康状况监视	Web 服务	Coh				
base_domain 由环境 一部署 日期务	保存 作	And													
女王初期 臣-互用性 臣-诊断	使用此贝P 查看 JNDI	使用此众可以就否该账券器的一般功能,例如以认补给通信。 查看 JNDI 树 @													
	名称:	名称:						AdminServer							
	模板:	模板:					(未指定值)更改							获取基本服务	
	🥂 计算机	🥂 计算机:					(无)							将要运行此用	
帮助主题	修 集群:	他 集群 :					(独立)							予器所属	
 配置默认网络连接 创建和配置计算机 	🦉 监听地	🦺 监听地址:												此服务器用于	
 配置集群 启动和停止服务器 	☑ 启用监	▶ 启用监听端口											指定是	星否可以	
 配置 WLDF 诊断数据量 应用服务器模板 	监听端口:	监听端口:					7001							5器用3	
系统指本	□ 启用 55	☑ 启用 SSL 监听端口					修改端口为默认的443								
正在运行的服务器的健康状况	SSL 监听崇	SSL 监听端口:					443							5器监印	
失败 (0) Critical (0)	日 🖧 启用	客户机证书作	理									指定	HttpClu		
Overloaded (0) 警告 (0)	Java 编译	Java 编译器:						javac							

ORACLE WebLogic Server 管理控制台 12c

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:





ORACLE WebLogic Server 管理控制台 12c												
更改中心	🏫 主页 注销 首选项 🔤 记录 帮助											
查看更改和重新启动	主页 >原务器探波 >AdminServer 省白											
启用配置编辑。将来在修改,添加或删除此 博由的项目时,将自动教廷这些事故。	▲ 已教活所有罪改。不需要更新自动。											
城市1900日间;村自动家有达三更快。	◆ 设置更新成功。											
域结构	AdminServer的沿来											
base_domain 申-环境												
部署												
一安全领域	一般信息集群服务 密制库 SSL 联合服务 部署 迁移 优化 超载 健康状况监视 服务器启动 Web服务											
世-ら用性 由-诊断	保存											
	8.99/年中以續保私有密钥和中間址书颁友机构(CA)的文字在發和管理。在此贝中,您可以宣誓和定义各种密钥库配置。这些设置有助于管理消息传输的文字。											
	密制版: 会制版记和 Java 标准信任 画改) → 洗 择标识和 JAVA 标准信任											
*R0h -> 85												
格明主题	c:\sslkeystore.jks											
 ·	定制标识密制库类型:											
• 间面密制库 • 设署 SSL	·····································											
	定制标识密钥库密码短语:											
系统状态	编记会制坛记奏组成李亮和语:											
正在运行的服务器的健康状况	朝鮮 9(7年 南136 小 2) 201年 2) m3/2 1日・											
Failed (0)	- 信任											
Critical (0) Overloaded (0)	Java 标准信任密钥库: C:\Orade\MIDDLE~1\JDK160~1\jre\Wb\security\cacerts											
Warning (0)	Java 标准信任密钥库类型: jus											
	Java 标准信任密钥库密码返语:											
	确认 Java 标准信任密钥库密码短语:											
	保存											
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"gdca",并输入私钥密码。修改完成后,记得要点击"保存"





AdminServer的设置																
配置	协议	日月	志记录	调试	监视	控制	部署	服务	安全	注释						
一般的	息	集群	服务	密钥库	SSL	联合	服务	部署	迁移	优化	超载	健康状况监视	服务器启动	Web 服务		
保存	保存															
在此	页中 , 1	您可以	查看和定	2义此服9	号器实例	的各种	安全套	接字层 (SSL) 设置	島。这些	设置有助	加于管理消息传输	的安全。			
标识利	1信任	位置:										密钥库 更改				
— 标识	į —															
私有著	朝位	置:										来自定制标识密	阴库			
私有家	朝别	名:														
												guca			жоты 	
6日 私	有密锁	膝码	短语:									•••••		1		
備	认私有	宇密钼	密码短误	吾:										🗲 证书	密码	
证书位	〕 置:											来自定制标识密	附库			
— 信日	— 信任 ——————————————————————————————————															
可信证	可信证书颁发机构: 来自 Java 标准信任密钥库															
─₽高	14 <u>8</u>															
1417																

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。

三、 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

备份好步骤一生成的 <u>www.domainame.com.jks</u>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。

四、 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。

