



广东省数字证书认证中心

GDCA 信鉴易® SSL 服务器证书部署指南

For JBoss4/5/6/7 版本

2015/11/23

目录

一、 部署前特别说明.....	3
二、 生成证书请求.....	3
1. 安装 JDK&JBoss（仅针对没有安装的用户）	3
2. 生成 keystore 文件	3
3. 生成证书请求文件(CSR)	5
三、 导入服务器证书.....	5
1. 获取服务器证书.....	5
2. 获取根证书和 CA 证书	6
1) 从邮件中获取:	6
2) 从 GDCA 官网下载	7
3. 查看 keystore 文件内容	9
4. 导入证书.....	9
1) 导入根证书	9
2) 导入 CA 证书.....	9
3) 导入服务器证书	10
四、 安装服务器证书.....	10
1. 配置 JBoss（操作前备份相应配置文件，以备错误时恢复）	11
1) JBoss4/5/6 版本:	11
2) JBoss 7 版本:	12
2. 访问测试.....	12
五、 服务器证书的备份及恢复.....	14
1. 服务器证书的备份.....	14
2. 服务器证书的恢复.....	14



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”)主要描述如何生成证书请求和如何将 SSL 服务器证书部署到 JBoss 服务器
2. 本部署指南的适用范围: JBoss4/5/6/7 版本, JBoss3 以下版本(含 JBoss 3)没有经过严格测试
3. JBoss 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, 但地址栏不会变绿色。
4. 本部署指南使用 testweb.95105813.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、生成证书请求

1. 安装 JDK&JBoss (仅针对没有安装的用户)

安装过程比较简单, 采取默认方式安装即可, 如有需要可以修改安装的目录。

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 或 JRE 下的 bin 目录, 运行 keytool 命令(示例中粗体部分为可自定义部分, 可根据实际配置情况相应修改)。

```
keytool -genkey -alias gdca -keyalg RSA -keysize 2048 -keystore D:\gdca.jks
```



```
C:\Users\dgh>keytool -genkey -alias gdca -keyalg RSA -keysize 2048 -keystore D:\gdca.jks
输入密钥库口令:  → 密码不回显
再次输入新口令: 
您的名字与姓氏是什么?
[Unknown]: testweb.95105813.cn
您的组织单位名称是什么?
[Unknown]: 工程部
您的组织名称是什么?
[Unknown]: 广东数字证书认证中心有限公司
您所在的城市或区域名称是什么?
[Unknown]: 佛山市
您所在的省/市/自治区名称是什么?
[Unknown]: 广东省
该单位的双字母国家/地区代码是什么?
[Unknown]: CN
CN=testweb.95105813.cn, OU=工程部, O=广东数字证书认证中心有限公司, L=佛山市, ST=广东省, C=CN是否正确?
[否]: y

输入 <gdca> 的密钥口令
(如果和密钥库口令相同, 按回车):  → 直接按回车键

C:\Users\dgh>
```

(JDK 6 及以上版本, 密码输入时不会回显)

```
C:\Users\dgh>keytool -genkey -alias gdca -keyalg RSA -keysize 2048 -keystore D:\gdca.jks
输入 keystore 密码: password123 → 密码明文显示
您的名字与姓氏是什么?
[Unknown]: testweb.95105813.cn
您的组织单位名称是什么?
[Unknown]: 工程部
您的组织名称是什么?
[Unknown]: 广东数字证书认证中心有限公司
您所在的城市或区域名称是什么?
[Unknown]: 佛山市
您所在的州或省份名称是什么?
[Unknown]: 广东省
该单位的两字母国家代码是什么?
[Unknown]: CN
CN=testweb.95105813.cn, OU=工程部, O=广东数字证书认证中心有限公司, L=佛山市, ST=广东省, C=CN 正确吗?
[否]: y

输入 <gdca> 的主密码
(如果和 keystore 密码相同, 按回车):  → 直接按回车

C:\Users\dgh>
```

(JDK 5 版本, 密码明文显示)

以上命令中, gdca 为私钥别名(-alias), 生成的 gdca.jks 文件默认放在 D 盘根目录下。

注意:

- 请务必根据提示录入全部项目, 并保证其准确性



- 若输出路径含有空格，需使用英文状态下的双引号括起来
- keystore 密码至少 6 个字符，若电脑安装了 JDK 6 或以上版本，密码输入时不会显示；若安装了 JDK 5 版本，密码输入时将可能出现明文显示，请务必注意并牢记此密码，尤其含有大小写字母的情况
- 下文涉及到 keytool 工具输入的密码均为此密码
- 如组织名称含有逗号，录入时不用输入引号，一般系统会在下面提示信息中的组织名称自动添加引号，请务必查看；如发现没有引号，请关闭命令行窗口，然后打开一个新窗口重新操作；
- 提示输入主密码时直接按回车即可，保证 keystore 密码与 gdca 主密码一致

3. 生成证书请求文件(CSR)

```
keytool -certreq -alias gdca -sigalg SHA256withRSA -file D:\certreq.csr -keystore D:\gdca.jks
```



```
C:\Users\dgh>keytool -certreq -alias gdca -sigalg SHA256withRSA -file D:\certreq.csr -keystore D:\gdca.jks
输入 keystore 密码:
C:\Users\dgh>
```

请备份密钥库文件 gdca.jks，将证书请求文件 certreq.csr 提交给 GDCA，等待证书签发。如密钥库文件 gdca.jks 丢失，会导致证书不可用。

三、导入服务器证书

1. 获取服务器证书

在您完成申请 SSL 服务器证书的流程后，GDCA 将会在返回给您的邮件中附上服务器证书，请留意查看申请证书时填写的邮箱。



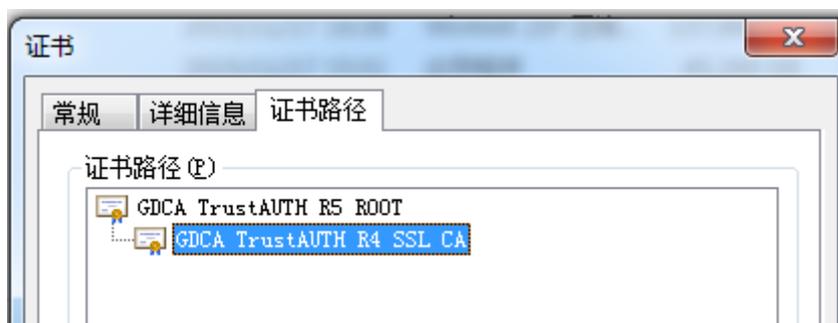
2. 获取根证书和 CA 证书

获取根证书和 CA 证书可参考以下两种方法之一，建议优先从邮件中获取。

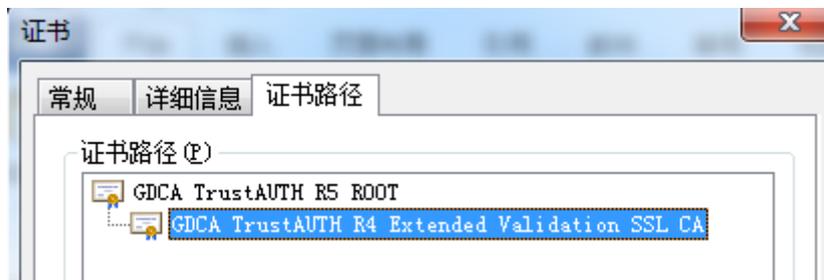
1) 从邮件中获取：

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根证书 GDCA_TrustAUTH_R5_ROOT.cer 和相应的 CA 证书，请留意查看申请证书时填写的邮箱。如果您申请的是睿信(OV) SSL 证书 (Organization Validation SSL Certificate)，CA 证书文件就是 GDCA_TrustAUTH_R4_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_Extended_Validation_SSL_CA.cer，请确认所收到的证书文件是您需要的 CA 证书。

GDCA_TrustAUTH_R4_SSL_CA.cer:



GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer:



2) 从 GDCA 官网下载

用户可以访问 GDCA 官网：<http://www.gdca.com.cn/channel/001002002>，下载服务器证书的根证书和 CA 证书，如下图所示：



获取第一张证书：根证书 GDCA_TrustAUTH_R5_ROOT.cer，如下图所示：

下载根证书

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）。

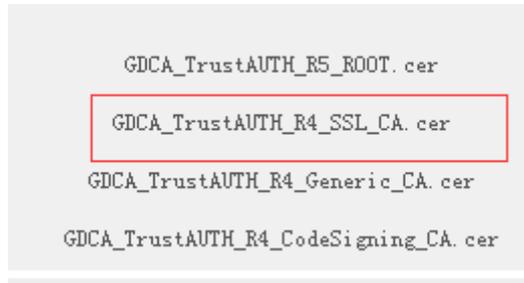
12 项，显示 1 到10. [首页/前一页] 1 2 [下一页/末页]

CA名称	起始有效时间	截止有效时间	CA证书下载
ROOTCA_sm2	2012-07-14 11:11:59	2042-07-07 11:11:59	社会公众应用根证书 (SM2).cer
GDCA TrustAUTH E1 CA	2014-06-26 15:02:11	2034-06-21 15:02:11	广东数字证书认证中心有限公司_sm2.cer
ROOTCA_rsa	2005-08-28 16:16:16	2025-08-23 16:16:16	社会公众应用根证书 (RSA).cer
GDCA TrustAUTH R2 CA	2013-12-16 14:29:40	2018-12-15 14:29:40	广东数字证书认证中心有限公司_rsa.cer
GDCA Root CA	2004-01-11 17:34:22	2024-12-11 00:00:00	GDCA_Root_CA.cer
GDCA Guangdong Certificate Authority	2004-01-12 10:13:07	2024-01-12 10:13:07	GDCA_Guangdong_Certificate_Authority.cer
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA_TrustAUTH_R5_ROOT.cer
GDCA TrustAUTH R4 SSL CA	2014-11-26 17:52:00	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_SSL_CA.cer
GDCA TrustAUTH R4 Generic CA	2014-11-26 17:53:00	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Generic_CA.cer
GDCA TrustAUTH R4 CodeSigning CA	2014-11-26 17:54:35	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_CodeSigning_CA.cer



获取第二张证书:

CA 证书若您申请的证书是睿信(OV) SSL 证书(Organization Validation SSL Certificate)，下载 GDCA_TrustAUTH_R4_SSL_CA.cer，如下图所示:

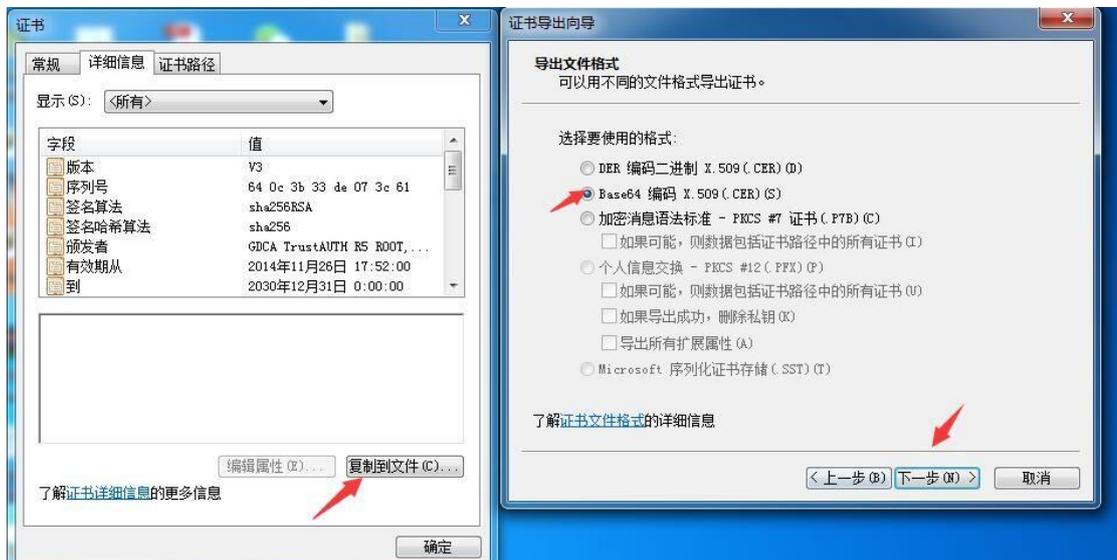


若您申请的证书是恒信企业 EV SSL 证书(Extended Validation SSL Certificate)，则下载 GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer

12 项, 显示 11 到12. [首页/前一页] 1, 2 [下一页/末页]

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R4 Extended Validation SSL CA	2014-11-26 17:45:25	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer

从 GDCA 官网获取根证书和 CA 证书后需要转换成 Base64 编码格式，如下图所示:



3. 查看 keystore 文件内容

进入 JDK 安装目录下的 bin 目录, 运行 `keytool -list -keystore d:\gdca.jks` 查询 keystore 文件信息。

```
C:\Users\dgh>keytool -list -keystore d:\gdca.jks
输入 keystore 密码:

Keystore 类型: JKS
Keystore 提供者: SUN

您的 keystore 包含 1 输入
gdca, 2015-10-29, PrivateKeyEntry, 或 KeyEntry
认证指纹 (MD5): 9D:58:CF:CE:7C:33:54:F5:96:31:75:29:FA:11:FE:C9

C:\Users\dgh>
```

4. 导入证书

1) 导入根证书

导入前将 GDCA TrustAUTH R5 ROOT.cer 文件改名为 ca1.cer, 用户可以修改为其他容易记忆的名字。

```
keytool -import -alias ca1 -keystore D:\gdca.jks -trustcacerts -file
D:\ca1.cer -noprompt
```

2) 导入 CA 证书

导入前将 GDCA TrustAUTH R4 Extended Validation SSL CA.cer 或 GDCA TrustAUTH R4 SSL CA.cer 文件改名为 ca2.cer, 用户可以修改为其他容易记忆的名字。

```
keytool -import -alias ca2 -keystore D:\gdca.jks -trustcacerts -file
D:\ca2.cer -noprompt
```



```
C:\Users\dgh>keytool -import -alias ca1 -keystore D:\gdca.jks -trustcacerts -file D:\ca1.cer -noprompt
输入 keystore 密码:
认证已添加至 keystore 中

C:\Users\dgh>keytool -import -alias ca2 -keystore D:\gdca.jks -trustcacerts -file D:\ca2.cer -noprompt
输入 keystore 密码:
认证已添加至 keystore 中

C:\Users\dgh>
```

3) 导入服务器证书

导入前将服务器证书文件 testweb.95105813.cn.cer 改名为 server.cer, 用户可以选择修改为其他容易记忆的名字或直接使用默认名字。

```
keytool -import -alias gdca -keystore D:\gdca.jks -trustcacerts -file D:\server.cer
```

```
C:\Users\dgh>keytool -import -alias gdca -keystore D:\gdca.jks -trustcacerts -file D:\server.cer
输入 keystore 密码:
认证回复已安装在 keystore 中 或证书回复已安装在密钥库中

C:\Users\dgh>
```

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。证书导入完成, 运行 `keytool -list -keystore D:\gdca.jks`, 查看 keystore 文件内容

```
C:\Users\dgh>keytool -list -keystore D:\gdca.jks
输入 keystore 密码:

Keystore 类型: JKS
Keystore 提供者: SUN

您的 keystore 包含 3 输入

ca2, 2015-10-29, trustedCertEntry,
认证指纹 (MD5): 63:CC:D9:3D:34:35:5C:6F:53:A3:E2:08:70:48:1F:B4
ca1, 2015-10-29, trustedCertEntry,
认证指纹 (MD5): 3E:DE:DB:4F:AA:05:02:A2:1C:9A:68:C0:A2:44:C0:DA
gdca, 2015-10-29, PrivateKeyEntry, 或KeyEntry
认证指纹 (MD5): AB:49:C4:0E:5E:51:F8:03:04:0C:6E:64:E2:C1:5E:60

C:\Users\dgh>
```

四、安装服务器证书



1. 配置 JBoss (操作前备份相应配置文件, 以备错误时恢复)

配置过程因 JBoss 版本不同稍有区别, 可参考下面进行配置。

1) JBoss4/5/6 版本:

复制已正确导入认证回复的 gdca. jks 文件到 JBoss 的 server\default\conf 目录, 使用文本编辑器打开 server.xml, 找到并修改以下内容:

<!--

```
<Connector port="8443"...../>
```

-->

默认情况下<Connector port="8443"...../>是被注释的, 配置时需把“<!-- -->”去掉, 然后对其节点进行相应的修改, 修改后如下所示:

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"port="443" address="${jboss.bind.address}"scheme="https"
secure="true" clientAuth="false"keystoreFile="${jboss.server.home.dir}/conf/gdca.jks"keystorePass="密钥库密码"
sslProtocol = "TLS" />
```

备注:

JBoss 4 版本: server.xml 文件默认存放在 JBoss 安装目录下
server\default\deploy\jboss-web.deployer

JBoss 5/6 版本: server.xml 文件默认存放在 JBoss 安装目录下
server\default\deploy\jbossweb.sar



2) JBoss 7 版本:

复制已正确导入认证回复的 gdca.jks 文件到 JBoss 的 standalone\configuration 目录下，使用文本编辑器打开 configuration 目录下的 standalone.xml 文件，找到以下节点：

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">
```

在该节点中新增一个 https 的链接器子节点：

```
<connector name="https" scheme="https" protocol="HTTP/1.1" socket-binding="https" secure="true"><ssl name="https"
password="密钥库密码" certificate-key-file="../../standalone/configuration/gdca.jks"/> </connector>
```

修改后如下图所示：

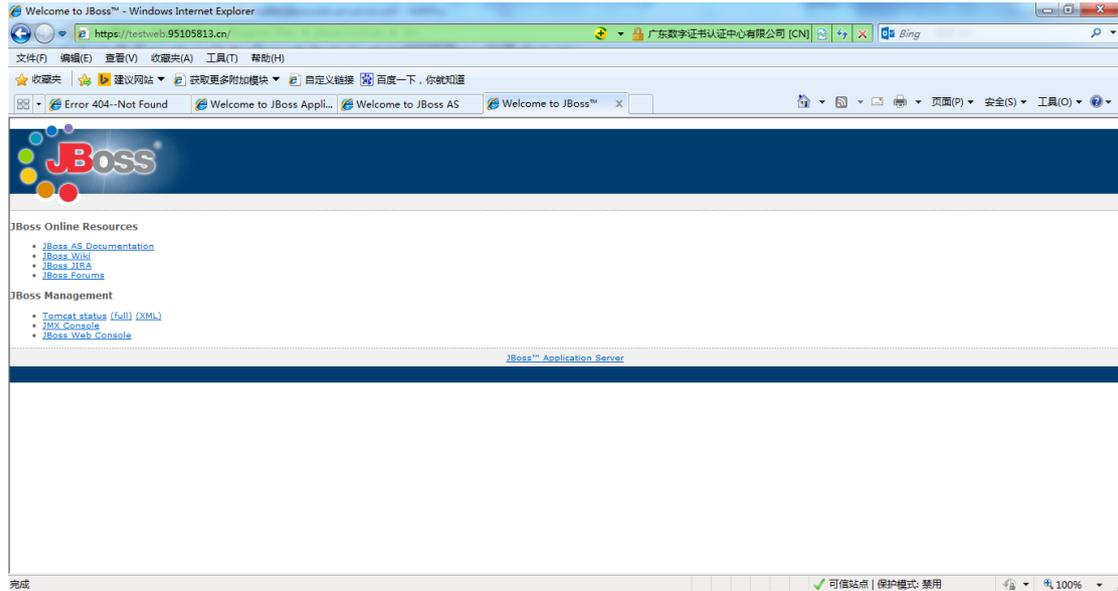
```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">
  <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
  <connector name="https" scheme="https" protocol="HTTP/1.1" socket-binding="https" secure="true">
    <ssl name="https" password="密钥库密码" certificate-key-file="../../standalone/configuration/gdca.jks"/>
  </connector>
  <virtual-server name="default-host" enable-welcome-root="true">
    <alias name="localhost"/>
    <alias name="example.com"/>
  </virtual-server>
</subsystem>
```

默认的 SSL 访问端口号为 443，如果使用其他端口号，则您需要使用 https://yourdomain:port 的方式来访问您的站点，防火墙要开放相应的 port。

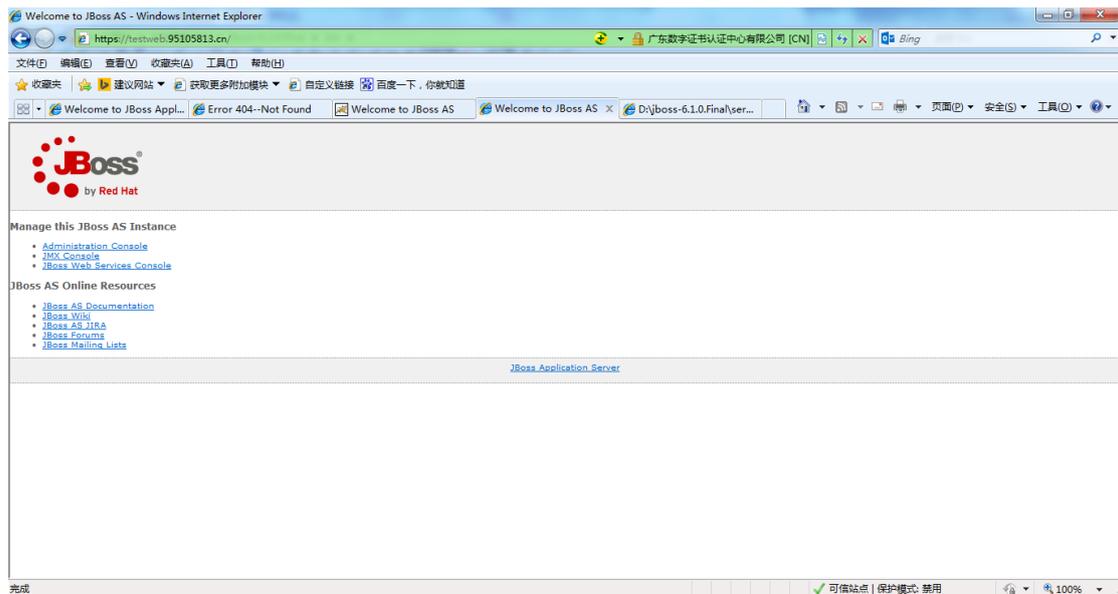
2. 访问测试

服务器若部署了睿信 SSL 证书，浏览器访问时将出现安全锁标志；若部署了恒信企业 EV SSL 证书，浏览器除了显示安全锁标志，地址栏会变成绿色，如下图：



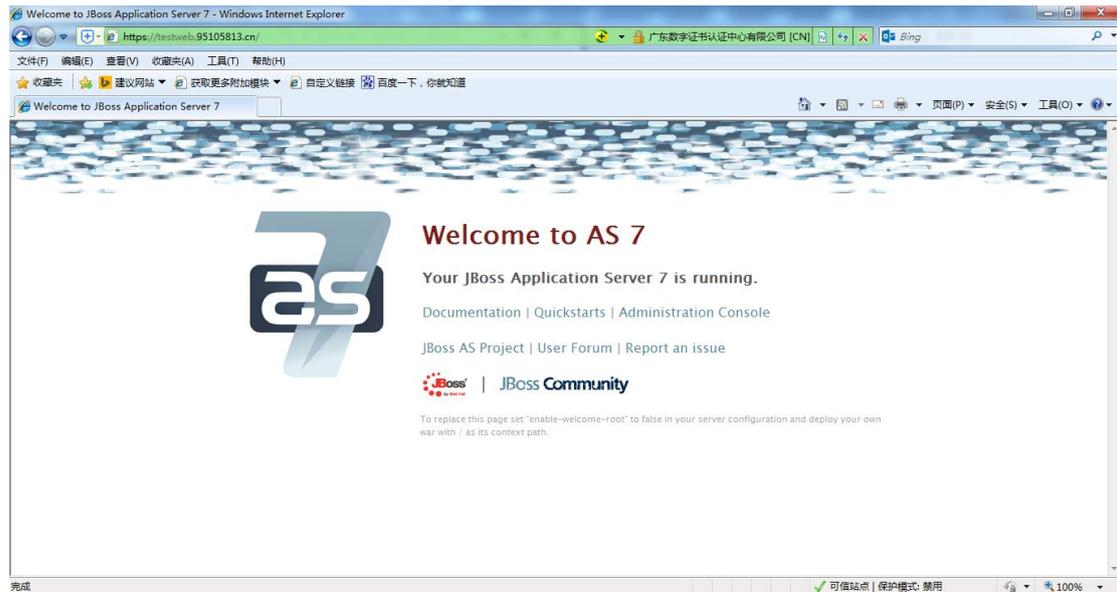


(JBoss4/5 访问效果)



(JBoss 6 访问效果)





(JBoss 7 访问效果)

五、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。

1. 服务器证书的备份

备份服务器证书密钥库文件 `gdca.jks` 文件即可完成服务器证书的备份操作。

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 `gdca.jks` 文件恢复到您的服务器上，并修改配置文件，恢复服务器证书的应用。若服务器证书丢失，请联系 GDCA 重新签发。

