



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 Resin 版

修订日期：2017/03/08

目录

一、	部署前特别说明.....	3
二、	生成证书请求.....	4
	1. 安装 OpenSSL 工具.....	4
	2. 生成服务器证书私钥.....	4
	3. 生成服务器证书请求 (CSR) 文件.....	5
	4. 提交证书请求.....	6
三、	安装 ssl 证书.....	7
	1. 获取证书公钥:	7
	2. Opessl 模式安装 ssl 证书.....	7
	3. JSSE 模式配置服务器证书.....	8
	4. 测试安装结果.....	9
四、	服务器证书的备份.....	9
五、	服务器证书的恢复.....	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: F5 负载均衡设备
3. Resin 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。
5. 如用户已经生成证书请求文件, 请从第三点导入服务器证书开始阅读。

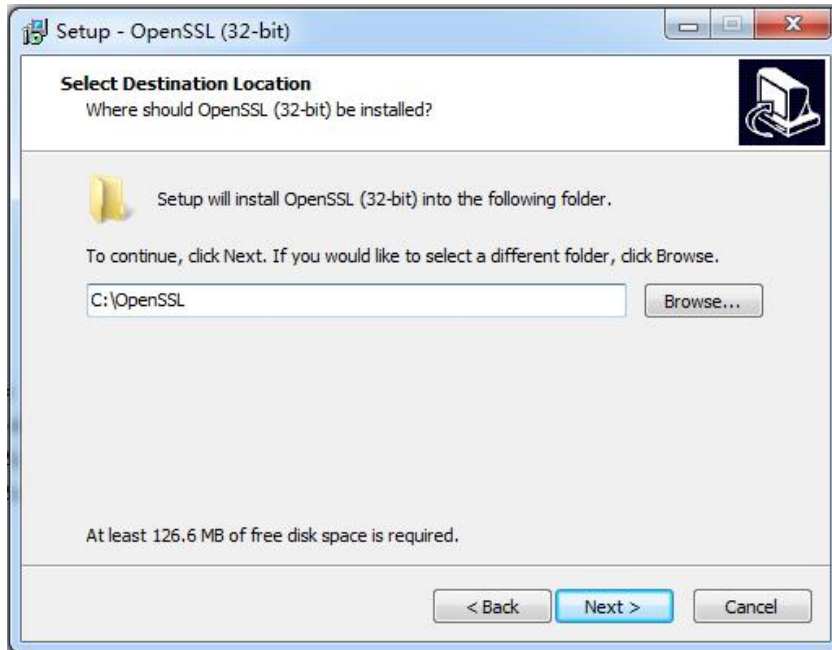


二、生成证书请求

1. 安装 OpenSSL 工具

您需要使用 Openssl 工具来创建证书请求。下载 OpenSSL:

<http://slproweb.com/products/Win32OpenSSL.html> 安装 OpenSSL 到 C:\OpenSSL



安装完后将 C:\OpenSSL\bin 目录下的 openssl.cfg 重命名为 openssl.cnf

2. 生成服务器证书私钥

命令行进入 C:\OpenSSL\bin，生成证书私钥。产生的私钥文件可以是 server.key 这样简单的命名或者使用我们推荐的使用主机域名方式进行命名。

```
cd c:\OpenSSL\bin
```

先设置环境变量

```
set OPENSSL_CONF=openssl.cnf
```

参考:

```
openssl genrsa -out server.key 2048
```

例:

```
openssl genrsa -out D:\testweb.95105813.cn.key 2048
```



```
ca. 管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>cd c:\OpenSSL\bin

c:\OpenSSL\bin>set OPENSSL_CONF=openssl.cnf

c:\OpenSSL\bin>openssl genrsa -out D:\testweb.95105813.cn.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

c:\OpenSSL\bin>
```

3. 生成服务器证书请求 (CSR) 文件

参考:

```
openssl req -new -key server.key -out certreq.csr
```

例:

```
openssl req -new -key D:\testweb.95105813.cn.key -out D:\certreq.csr
```

如出现以下报错请先设置环境变量

```
set OPENSSL_CONF=openssl.cnf
```

```
c:\OpenSSL\bin>openssl req -new -key D:\testweb.95105813.cn.key -out D:\certreq.csr
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Unable to load config info from /usr/local/ssl/openssl.cnf

c:\OpenSSL\bin>_
```

执行成功后提示要输入您的相关信息。填写说明:

1.Country Name:

填您所在国家的 ISO 标准代号, 如中国为 CN, 美国为 US

2.State or Province Name:

填您单位所在地省/自治区/直辖市, 如广东省或 Guangdong

3.Locality Name:

填您单位所在地的市/县/区, 如佛山市或 Foshan

4.Organization Name:

填您单位/机构/企业合法的名称, 如数安时代科技股份有限公司或 Global Digital Cybersecurity Authority Co., Ltd.

5.Organizational Unit Name:

填: 部门名称, 如技术支持部或 Technical support

6.Common Name:



填：域名，如：testweb.95105813.cn。在多个域名时，填主域名

7.Email Address:

填您的邮件地址，不必输入，按回车跳过

8.'extra'attributes

从信息开始的都不需要填写，按回车跳过直至命令执行完毕。

字段	说明	示例
Country Name	ISO 国家代码(两位字符)	CN
State or Province Name	所在省份	Guangdong
Locality Name	所在城市	Guangzhou
Organization Name	公司名称	Digital Cybersecurity Authority Co., Ltd.
Common Name	申请证书的域名	www.trustauth.cn
Email Address	不需要输入	
A challenge password	不需要输入	
Anoptionalcompany name	不需要输入	

```

管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>openssl req -new -key E:\testweb.key -out E:\certreq.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:CN
State or Province Name (full name) []:广东省
Locality Name (eg, city) []:佛山市
Organization Name (eg, company) []:数安时代科技股份有限公司
Organizational Unit Name (eg, section) []:安全管理部
Common Name (eg, your websites domain name) []:testweb.gdca.com.cn
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:

C:\Users\Administrator>_
半:
    
```

除第 1、6、7、8 项外，2-5 的信息填写请统一使用中文或者英文填写。并确保您填写的所有内容和您提交到 GDCA 的内容一致，以保证 SSL 证书的签发。

4. 提交证书请求

请您保存证书私钥文件 testweb.95105813.cn.key，最好复制一份以上副本到不同的物理环境上（如不同的主机），防止丢失。并将证书请求文件 certreq.csr 提交给 GDCA。



三、 安装 ssl 证书

Resin 目前最新的版本还是 4.0 (4.0.49)，使用 Java EE6，在 Resin 上部署证书，一般有两种方式，首先我们推荐采用 Openssl 方式，不仅因为 Openssl 模式下的速度更快，而且 Openssl 对 TLS 的支持更好，安全性高；另外一种 JSSE 方式，不仅速度慢，而且 JSSE6 仅支持 TLS1.0

1. 获取证书公钥：

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_OV_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_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)



2. Openssl 模式安装 ssl 证书

打开 Resin.xml，增加下面配置：



```
<resin xmlns="http://caucho.com/ns/resin">
  <cluster id="http-tier">

    <server id="a" address="192.168.1.12">
      <http port="443">
        <openssl>
          <certificate-file>keys/server.crt</certificate-file>
          <certificate-key-file>keys/server.key</certificate-key-file>
          <password>my-password</password>
          <certificate-chain-file>keys/chain.crt</certificate-chain-file>
          <cipher-suite>ALL:!ADH:+HIGH:+MEDIUM:!NULL:!DH:!RC4:!DES" </cipher-suite>
          <protocol>tlsv1 tls1.1 tls1.2</protocol>
        </openssl>
      </http>
    </server>

    ...
  </resin>
```

说明:

<certificate-file>: 服务器证书文件。

<certificate-key-file>: 服务器证书的私钥文件。

<password>: 服务器证书私钥文件的密码, 如果原私钥文件没有密码, 可以运行如下 openssl 命令:

```
openssl rsa -in server.key -des -out serverpass.key -passout pass:123456
```

<certificate-chain-file>: 中间证书文件。

<cipher-suite>: 加密套件设定。

<protocol>: 协议说明, 一般只打开 TLS 1, TLS 1.1, TLS 1.2 协议。

3. JSSE 模式配置服务器证书

打开 resin.xml, 增加以下参数:

```
<resin xmlns="http://caucho.com/ns/resin">
  <cluster id="">
    <server-default>
      <http port="443">
        <jsse-ssl>
          <key-store-type>jks</key-store-type>
          <key-store-file>keys/server.keystore</key-store-file>
          <password>changeit</password>
```




```
<protocol>-sslv3</protocol>  
</jsse-ssl>  
</http>  
</server-default>  
...  
</cluster>  
</resin>
```

说明:

<key-store-type>: 设定 Keystore 文件的类型, 这里一般都设为 jks。

<key-store-file>: JKS 文件名。

<password>: JKS 文件的密码。

<protocol>: 支持的协议。测试 SSL 证书

4. 测试安装结果

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> 的方式来访问您的站点, 防火墙要开放相应的 port。

四、 服务器证书的备份

备份服务器证书私钥文件 `testweb.95105813.cn.key`, 服务器证书文件 `testweb.95105813.cn.crt`, 即可完成服务器证书的备份操作。

五、 服务器证书的恢复

参照步骤“三、安装服务器证书”即可完成恢复操作

