广东省数字证书认证中心

GDCA 信鉴易® TrustAUTH®证书常见问题解答

2015/11/23

GDCA 信鉴易® TrustAUTH®证书常见问题解答

目录

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

证书部署阶段常见问题

一、 在配置 apache 或 Nginx 时，可以使用 cer 格式的服务器证书吗？

在 apache 和 Nginx 上可以使用 cer 格式的服务器证书，但需要将证书的编码转换成 Base64 编码。

二、 Windows Server IIS 配置常见问题

（一）、IIS7.0 禁用 SSL2.0 和 SSL3.0 协议

Windows Server 2008 /2012 中使用 IIS 7 /8 默认允许 SSL 2.0 和 SSL 3.0，下面介绍怎样关闭不安全的 SSL 2.0 和 SSL3.0 协议，可按如下操作：

1、 单击开始，单击运行，键入注册表编辑器，然后单击确定。

2、在注册表编辑器，找到以下注册表项/文件夹：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols

3、在 SSL 2.0 文件夹，右键单击并选择新建，然后单击项(K)。然后重命名文件夹为：Server。

4、 右键点击 Sever 的文件夹，选择新建，然后单击 DWORD（32-bit）值。

5、 将新建的 DWORD 重命名为：Enabled ，并按下回车键。

6、请确保它显示 00000000（0）。如果没有，请右键单击并选择修改，输入 0 作为数值数据。

7、现在，禁用 SSL 3.0，对 SSL 3.0 文件夹，右键单击并选择新建，然后单击项(K)。命名新的文件夹为：Server。

8、 右键点击 Sever 的文件夹，选择新建，然后单击 DWORD（32-bit）值。

9、 将新建的 DWORD 重命名为：Enabled，并按下回车键。

10、请确保它显示 00000000（0）的数据列下。如果没有，请右键单击并选择修改，输入 0 作为数值数据。

11、 重新启动计算机。

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

12、验证 SSL 2.0 或者 SSL 3.0 协议是否关闭请到 SSLLABS 网站体检

（二）windows server2003 版本 IIS6.0 不支持 sha256 算法

因为某部分 windows server2003 的版本上 IIS6.0 不支持 sha256 的算法，所以如果出现这个情况，请下载补丁编号 KB968730，安装到 win2003 上再进行操作。

（三）IIS7.0 搭载服务器备份需要注意什么？

备份可以从 IIS 软件中导出一个.PFX 文件后进行保存，如果要重新恢复的话只需要重新导入该文件即可。

三、Windows Server Tomcat 配置常见问题

(一)、客户端访问部署了 EV SSL 证书的 web 应用，有安全锁图标，但地址栏是白色的，没有变绿？

请参考以下排查：

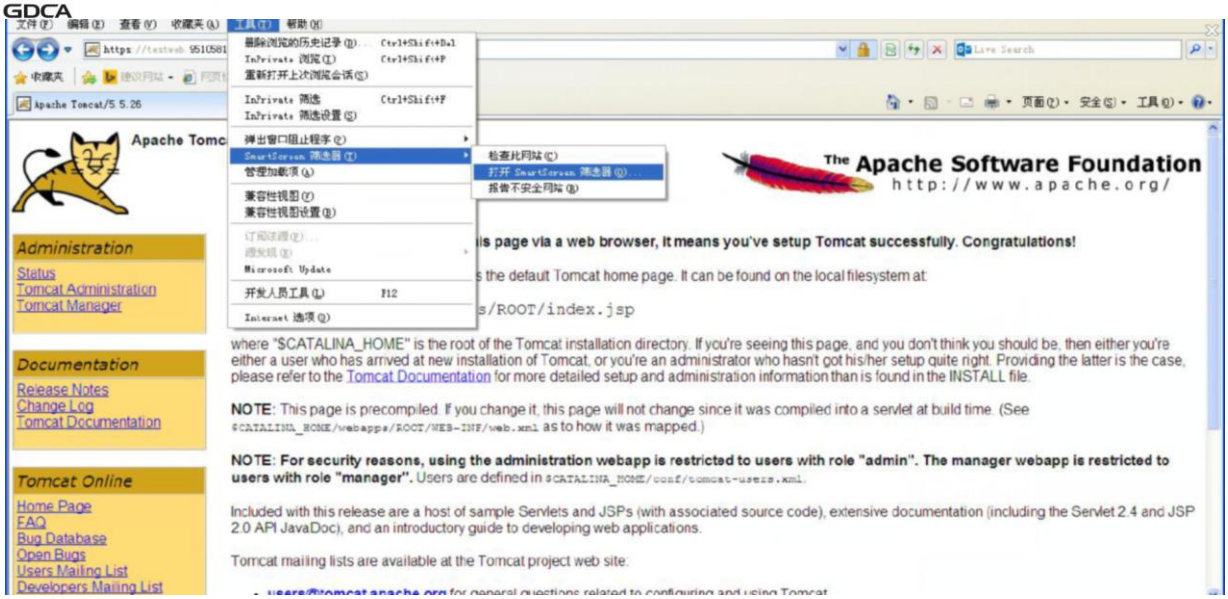
- 如您电脑环境是 Windows XP 操作系统，IE7 以上浏览器，请参考下图启用 SmartScreen 筛选器后重新打开浏览器访问：
- Windows XP 或其他 Windows 操作系统，重置浏览器再试。

下图一：有安全锁图标，但地址栏是白色的

下图二：请按图示进行相关设置；

下图三：显示正常后的图示

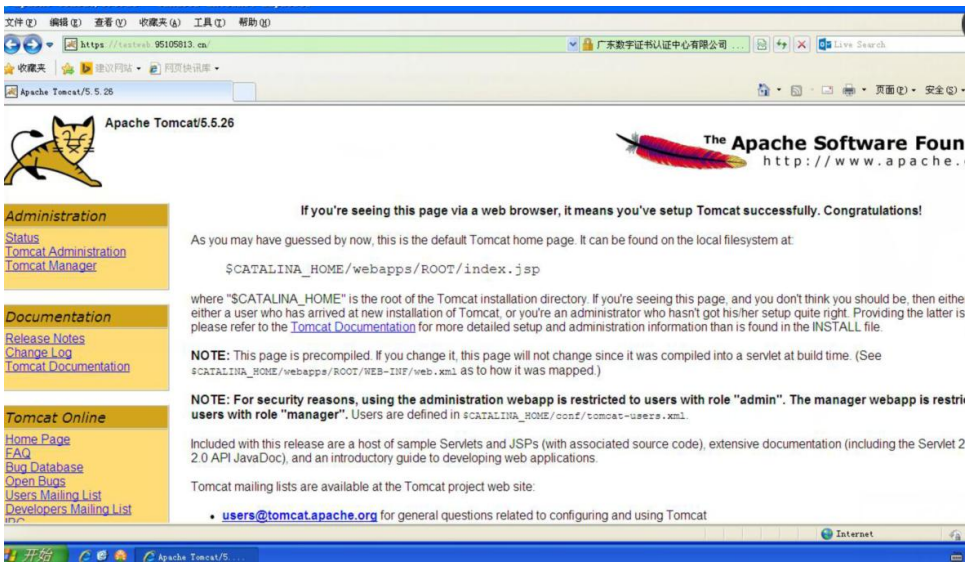
地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813



上图为图一

上图为图二

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813



上图为图三

四、如何使用 keystore.jks 转换为 apache、nginx 使用的 key 和 crt 文件？

1、从 JKS 转换到 PKCS12

keytool -importkeystore -srckeystore D:\keystore.jks -destkeystore D:\keystore.p12 -srcstoretype JKS -deststoretype PKCS12 -srcstorepass 123456 -deststorepass 123456 -srcalias testweb -destalias testweb -srckeypass 123456 -destkeypass 123456 -noprompt

```
c:\Java\jdk1.6.0_45\bin>keytool -importkeystore -srckeystore D:\keystore.jks -de
stkeystore D:\keystore.p12 -srcstoretype JKS -deststoretype PKCS12 -srcstorepass
 123456 -deststorepass 123456 -srcalias testweb -destalias testweb -srckeypass 1
23456 -destkeypass 123456 -noprompt
```

2、从 PKCS12 转换成 PEM 格式

openssl pkcs12 -in D:\keystore.p12 -out D:\testweb.gdca.com.cn.pem -passin pass:123456 -passout pass:123456

```
c:\OpenSSL\bin>openssl pkcs12 -in D:\keystore.p12 -out D:\testweb.gdca.com.cn.pe
m -passin pass:123456 -passout pass:123456
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
MAC verified OK
```

3、用记事本打开 PEM 格式文件，将“-----BEGIN ENCRYPTED PRIVATE KEY-----”至“-----END ENCRYPTED PRIVATE KEY-----”的内容拷贝出来，保存为

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

testweb.95105813.cn.key，至此私钥提取成功。

4、服务器证书和证书链也可以在 testweb.gdca.com.cn.pem 提取出来，然后保存成 crt 文件。

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813