Tomcat 配置 https 单向认证

ssl https tomcat

单向认证

生成密钥库和证书使用JDK提供的 keytool 工具，在 jdk 的 bin 目录下。在此，以windows为例。。。

生成密钥库

在cmd下，进入到 jdk bin目录，执行以下代码:

```
keytool -genkey -validity 36000 -alias www.xiaozhi.com -keyalg RSA -keystore d:\xiaozhi.keystore
```

控制台输出

> 在这里密钥库的密码我用的是“123456”，此密码在Tomcat配置时会用到
> 密钥库包含私钥和公钥等文件。把它用于服务器端的证书库，用于客户端浏览器认证服务端。
> **alias 和 ″名字与姓氏″ 并不是随便写的，而是域名或者IP。**

导出证书

光有keyStore文件是不够的，还需要证书文件，证书才是直接提供给外界使用的公钥凭证。

```
keytool -export -keystore d:\xiaozhi.keystore -alias www.xiaozhi.com -file d:\xiaozhi.cer -rfc
```

Tomcat 配置

本例为apache-tomcat-7.0.69。打开server.xml ， 打开https的注释，并修改为如下：

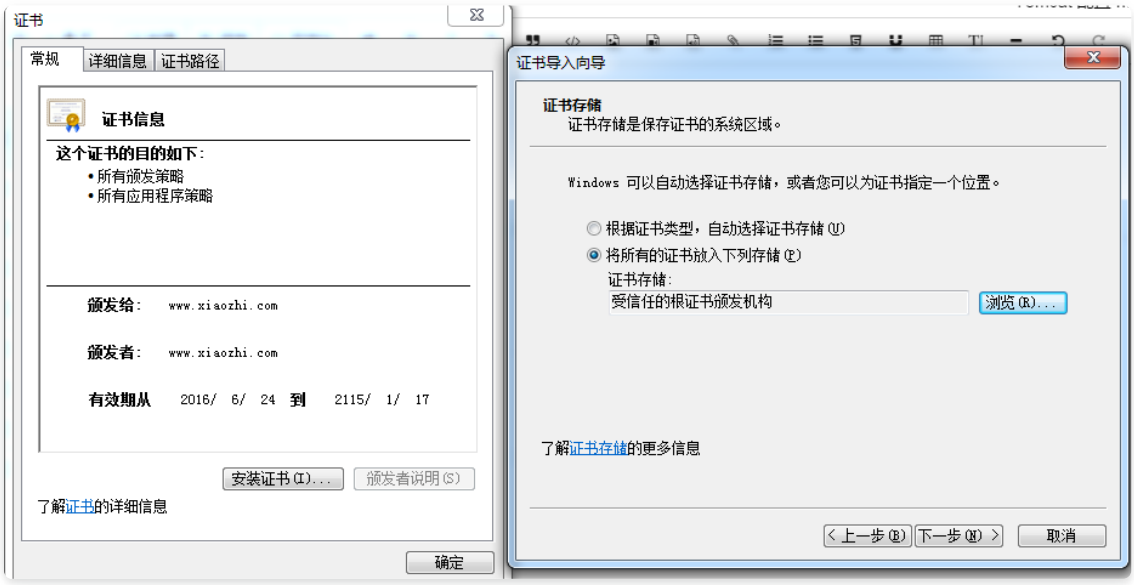
```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
               maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
               keystoreFile="d:\xiaozhi.keystore"
               keystorePass="123456"/>
```

> clientAuth为是否验证客户端，双向认证时改为 true

客户端安装证书

有两种方式安装，分别如下：

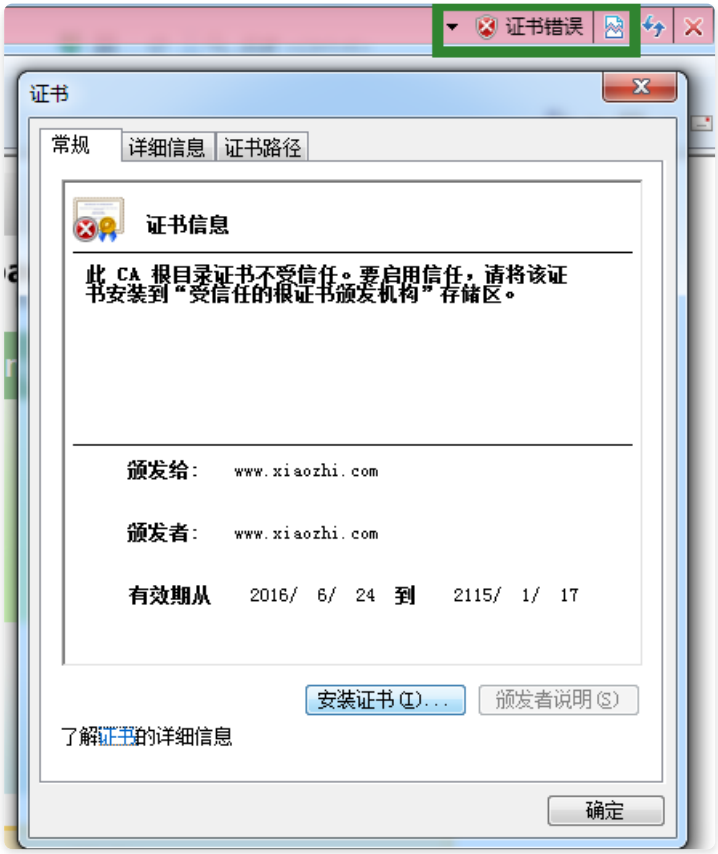
1. 将上步导出的证书发送给客户端，客户端可直接双击安装，安装到 “ 受信任的根证书颁发机构 ” 下。



证书安装

2. 在浏览器中向服务器发送请求，服务器会将证书发送回客户端，客户端再选择安装证书，安装完成后重启浏览器。

以不安全的方式浏览网站



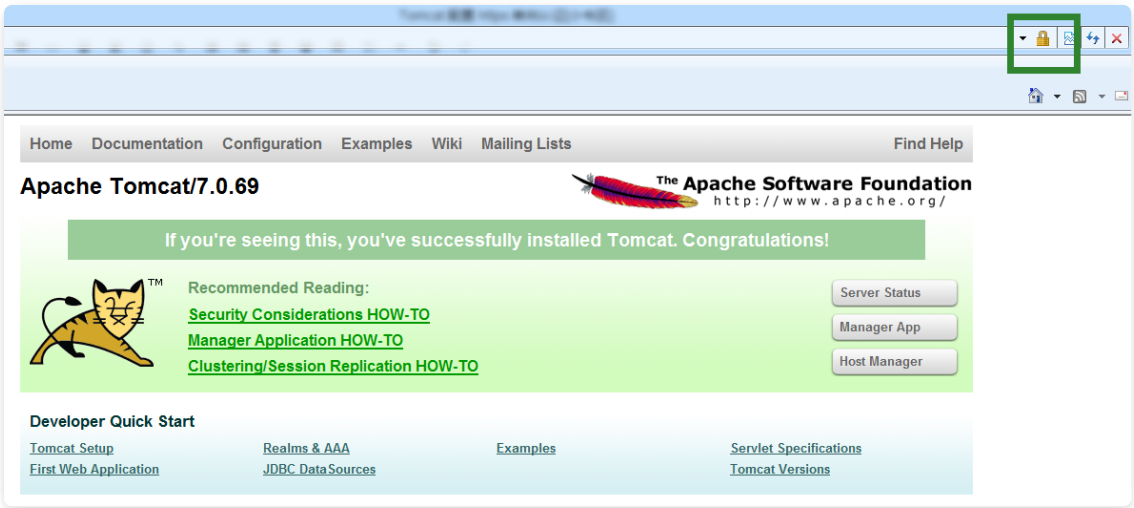
安装服务器返回的证书

验证

更改hosts文件，进行域名映射，此处如下：

```
127.0.0.1 www.xiaozhi.com
```

证书安装完成后，重启浏览器，输入请求地址(https://www.xiaozhi.com:8443/)，能正确打开即为正确。如下图:



安装成功示例

参考文档

1. Java加密技术（八）——数字证书
2. https单向认证和双向认证