秋明分享平台之

**CentOS下配置nginx的https代理**

撰稿人：秋明

撰稿人邮箱：tyumen@zhoufengjie.cn

QQ群：90122290、68610841【朋友建的一个群，包括你有什么比较不错的群也可以联系我放到这里】

本文撰稿日期： 2015年3月11日星期三

本站口号：开源、分享、共进

注解：任何想通过本平台分享文档的，可以随时联系，文档里面注明出稿人和邮箱，方便文档使用者同撰稿的兄弟技术咨询沟通和交流；

目录

1 前言 3

2 tomcat安装 3

3 证书生成 3

3.1 生成服务器端证书 3

3.2 生成导入证书(可以不关注) 4

3.3 为客户端生成证书 4

3.4 使服务器信任证书 5

4 tomcat配置 6

4.1 修改虚拟主机名 6

4.2 配置证书 6

5 访问测试 7

5.1 客户导入证书 8

5.2 浏览器访问测试 8

# 前言

https分单向认证和双向认证，作为单向认证，实际上就是只在server端做好证书，对客户端不进行认证；而双向认证必须在客户端导入证书之后，才能访问网站；

本文是讲解双向认证的配置方法，配置了双向认证之后，必须注意客户端需要导入证书之后才能访问网站；

# tomcat安装

这里忽略，朋友是装的7.0.42，所以我在官网下了一个7系列最新的版本，为了方便我这边跟朋友的目录一致，我安装的目录为：/opt/apache-tomcat-7.0.59

# 证书生成

做博客，网站等通常使用的是单向认证，这里为了简单可理解，自己生成一个证书来使用；

* 1. 生成服务器端证书

用于在tomcat上面进行配置的单向认证证书：

#mkdir /opt/apache-tomcat-7.0.59/conf/ssl && cd /opt/apache-tomcat-7.0.59/conf/ssl

# keytool -genkey -v -alias zhoufengjie.cn -keyalg RSA -validity 3650 -keystore www.zhoufengjie.cn.keystore -dname "CN=www.zhoufengjie.cn,OU=SinoCache,O=DevOpt,L=ChaoYang,ST=BeiJing,c=CN" -storepass Password -keypass Password

-dname参数说明：-dname "CN=(名字与姓氏), OU=(组织单位名称), O=(组织名称), L=(城市或区域名称), ST=(州或省份名称), C=(单位的两字母国家代码)"

* 1. 生成导入证书(可以不关注)

这一步有点多此一举，可以跳过；就是用户导入到浏览器中用于信任的客户端证书，在双向建联之后开始访问的时候会弹出网站信任，在浏览器提示的时候只需要点击下信任访问即可，或者把此证书导入到浏览器；

#keytool -export -alias zhoufengjie.cn -keystore www.zhoufengjie.cn.keystore -file www.zhoufengjie.cn.cer -storepass Password

* 1. 为客户端生成证书

下一步是为浏览器生成证书，以便让服务器来验证它。为了能将证书顺利导入至IE 和 Firefox ，证书格式应该是 PKCS12 ，因此，使用如下命令生成：

# keytool -genkey -v -alias zhoufengjie.cn -keyalg RSA -storetype PKCS12  -validity 3650 -keystore client.www.zhoufengjie.cn.p12 -dname "CN=www.zhoufengjie.cn,OU=SinoCache,O=DevOpt,L=ChaoYang,ST=BeiJing,c=CN" -storepass Password -keypass Password

* 1. 使服务器信任证书

由于是双向SSL 认证，服务器必须要信任客户端证书，因此，必须把客户端证书添加为服务器的信任认证。由于不能直接将 PKCS12 格式的证书库导入，我们必须先把客户端证书导出为一个单独的 CER 文件，使用如下命令：

# keytool -export -alias zhoufengjie.cn -keystore client.www.zhoufengjie.cn.p12 -storetype PKCS12 -storepass Password -rfc -file client.www.zhoufengjie.cn.cer

通过以上命令，客户端证书就被我们导出到“client.www.zhoufengjie.cn.cer ”文件了。下一步，是将该文件导入到服务器的证书库，添加为一个信任证书（在这一步中，会提示询问是否信任此证书，输入：yes回车）：

# keytool -import -v -file client.www.zhoufengjie.cn.cer -keystore www.zhoufengjie.cn.keystore -storepass Password

通过list 命令查看服务器的证书库，我们可以看到两个输入，一个是服务器证书，一个是受信任的客户端证书：

# keytool -list -keystore www.zhoufengjie.cn.keystore -storepass Password

# tomcat配置

tomcat配置方面比较简单，只需要配置一下server.xml即可；

* 1. 修改虚拟主机名

# vi /opt/apache-tomcat-7.0.59/conf/server.xml

修改defaultHost,找到如下行：

<Engine name="Catalina" defaultHost="www.zhoufengjie.cn">

修改webapps host，找到并修改如下行：

<Host name="www.zhoufengjie.cn" appBase="webapps"

* 1. 配置证书

# vi /opt/apache-tomcat-7.0.59/conf/server.xml

搜索8443，找到8443的配置，在下面添加如下的内容：

<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="true" sslProtocol="TLS"

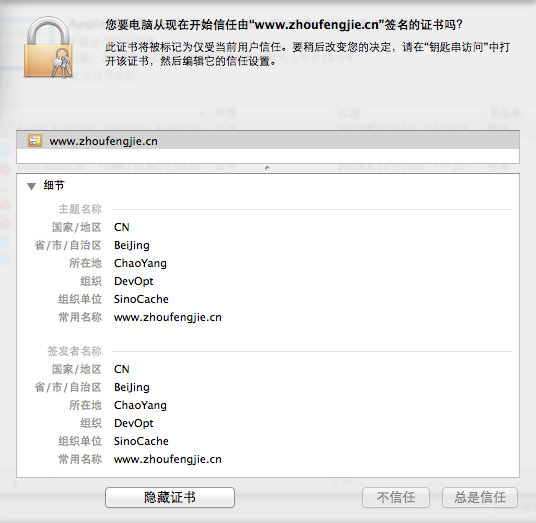
keystoreFile="conf/ssl/www.zhoufengjie.cn.keystore" keystorePass="Password"

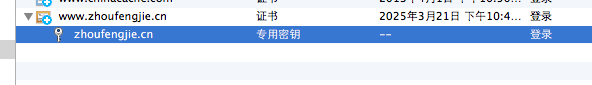
truststoreFile="conf/ssl/www.zhoufengjie.cn.keystore" truststorePass="Password"/>

# 访问测试

重启tomcat进程，使server证书生效；

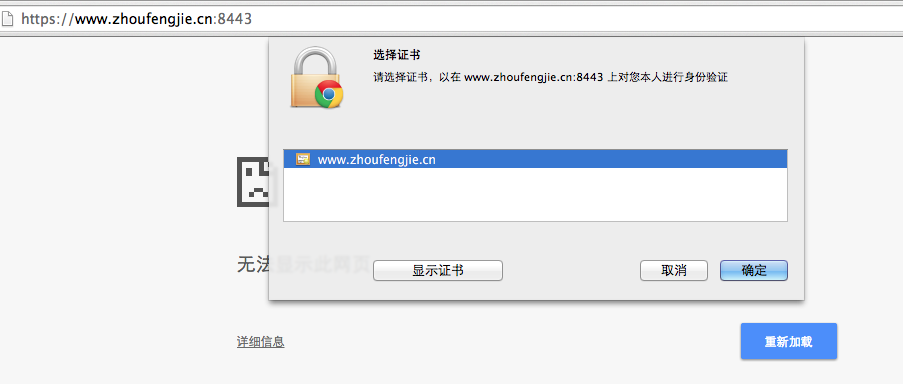
* 1. 客户导入证书





* 1. 浏览器访问测试

https://www.zhoufengjie.cn:8443，提示选择证书，选择确定：



然后提示私密连接，点击信任，查看测试结果，出现猫之后就说明你成功了；



