

【教程】如何申请 wosign 免费个人证书并 应用到阿里云服务器上的 tomcat

- 作者:zjhch123
- 原文链接: https://ld246.com/article/1462640833122
- 来源网站:链滴
- 许可协议: 署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

>0.拥有一个域名www.example.xxx并解析到阿里云服务器上

1.注册wosign账号

2.申请个人证书: "https://buy.wosign.com/free/"

3.域名验证

<方>之前wosign好像是需要手机号和域名注册人的信息,现在需要将一个文件上传至域名的根目录 者是使用域名邮箱进行验证,这里我们选择"上传文件至根目录"的方式。 上传文件至根目录后,即可进行验证。

<但是阿里云并不允许用户直接通过域名访问未备案的服务器,所以首先我们得先“伪造&r quo;一个https的url出来。何为伪造?就是自己给自己颁发https证书,以暂时绕过阿里云的验证,但 这种通过"伪造"方式使用https访问的网站会被大部分浏览器拦截,原因是自己颁发 自己的证书被浏览器认为是"不安全的证书"。(所以我称其为"伪造"htt s)

>具体过程就是:

ssh连接上服务器之后,选择一个目录,假定就是/root目录,在该目录下执行命令 keytool -genkey -alias tomcat -keyalg RSA

<方>之后会提示让你输入秘钥库密码,这里假定是"password",再会要求输入一些信息,大概是单名称省份城市国家之类的,可以随便输。之后会要求输入秘钥密码假定是"password"与秘钥库密码致。

完成之后去到xxxx/tomcat/conf/server.xml启用 SSL HTTP/1.1 连接器(已有配置,去除注释可),端口 改为443。

大概是这样的代码,去掉注释,修改端口就可以了

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

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

<然后增加以下两项。修改完成后的应该是这样</p>

<Connector port="443" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keyst reFile="/root/.keystore(这里是假定的目录)" keystorePass="password(这里是假定的密码)"/>< pre>

>并且修改Connector为以下形式

<Connector port="8080" protocol="org.apache.coyote.http11.Ht p11NioProtocol"

connectionTimeout="20000"

redirectPort="443(修改此处)" />

>重启完成后,可以开始进行wosign的验证,应该一次就能通过。

4.下载证书文件

<域名验证通过之后会让你设置证书的密码,这里假定是"PASSWORD"。设置完成后将wosign帮打包好的文件下载下来并妥善保管。</p>

5.设置服务器证书

将下载下来的证书文件解压,期间会让你输入解压密码,即刚才设置的证书的密码"PAS WORD",解压完成后,将其中"for Tomcat.zip"解压,得到xxxxx.jks文件,将该.jks文件上 至第三部假定的目录(这里是/root)内。

<网上有很多教程是说将tomcat的keystoreFile更改一下就可以使用https访问了,但是我最开始时候怎么也设置不对,之后按照如下的办法才设置成功,这里分享给大家。</p>

 i.查看一下证书库中的所有证书: keytool -li t 输入秘钥库密码password(第2步设置的假定密码) 此时会显示出已有证书,如果每一步都按照我的教程做, 显示有一个名叫"tomcat"的证书。

 ii 导入.jks的证书到现有的证书库中:keytool -importkeystore -srckeystore www.mbaoceancontent. om.jks 这里会让你输入原有秘钥库的密码"password"(假定),jks秘钥库的密码"PASSWORD"(假定)</pan>

 iii

删除"tomcat"秘钥 :keytool -delete -alias tomcat , 输入口令"password"

 iii .查询现有证书的名称:keytool -list 假定查询到的名称是"1"

 iii i.更改现有证书的名称为"tomcat":keytool -changealias -alias 1 -destalias tomcat 输入口令"passw rd"

 iii ii.更改现有秘钥的秘钥口令 :keytool -keypasswd -alias tomcat 输入口令"password" 输入原秘钥口 "PASSWORD" 输入新秘钥口令"password"

>之后,重启tomcat,即可安全无阻的访问https://www.example.xxx

至此,给服务器设置https访问就完成了。