链滴

tomcat 配置 Let'"'"'s Encrypt 多域名免费证书 centos 6.5

作者：Jacker
原文链接：https://ld246.com/article/1497605239743
来源网站：链滴

本文出现的意图

由于公司最近因为IOS版本的升级，开始全面推广https，所有的IOS客户端都要使用ssl证书。公司买阿里的证书一年要五千多，

感觉还是挺贵的。后来去了解原来还有免费证书这个东西，就想着去捣鼓一下，网上教程很多，标准一，大致都差不多。由于

每个机器的环境都不一样，导致遇到的情况也是不太一样。对于不少人来说，问题还是挺多的。如果伙不想自己去配置，可以

下载宝塔的面板来管理网站，它就有一键部署Let's Encrypt 的功能，我在腾讯云下使用宝塔没有出现题，大家也可以用他来建站。

宝塔官网：点击跳转

配置 Let's Encrypt 免费证书的准备

1、 首先把你的域名解析到这台服务器，这里是多域名配置，那至少解析两个子域名过来啦，我这里析的是 ssl.huiyanxian.cn ，

tssl.huiyanxian.cn 切记是A解析啊

2、 首先你要配置好你的java环境，包括jdk，tomcat的安装。我的端口改为了80，具体配置如下（以不按照我的来配置）

```
<Connector port="80" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="44
" />

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150" sche
e="https"
    secure="true" keystoreFile="生成证书的路径" keystorePass="证书的密码"
      clientAuth="false" sslProtocol="TLS" />
```

3、 因为在安装过程中需要安装不少依赖，因为默认源在国外，导致依赖失败，所以需要先把源改为内源，大家可以用网易163的源，

或者阿里的，我这里用的是阿里的源，具体更换方法参考我前面的另一片文章 https://blog.huiyaxian.cn/articles/2017/06/15/1497490831833.html

4、 这里是使用的是certbot-auto 来申请证书，python要升级到2.7，centos 6.5 默认的python版是 2.6.6,升级python参考文章

(https://blog.fazero.me/2016/10/13/centos-update-python/)，这里提供了一键脚本，以及把pp升级到了最新。

开始安装

1、 安装 certbot

wget https://dl.eff.org/certbot-auto

chmod a+x certbot-auto

2、 申请ssl ，因为要验证你的域名是否解析到了你的服务器，会借用你的80/443端口。所以在执行面语句之前保证80/443

是没有被占用的。我这里只需要关闭tomcat就行。

./certbot-auto certonly --standalone --email xxxxxx@qq.com -d ssl.huiyanxian.cn -d tssl.huianxian.cn

这里是多域名的，想要在添加域名的话继续在后面添加 -d 域名 email后面填写的是你的邮箱

弹出的 两个选项 一个选择同意 A 另外一个选择 Y 就行。

等待到最后出现以下内容说明申请成功

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/ssl.huiyanxian.cn/fullchain.pem. Your cert
   will expire on 2017-09-14. To obtain a new or tweaked version of
   this certificate in the future, simply run certbot-auto again. To
   non-interactively renew *all* of your certificates, run
   "certbot-auto renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

说明申请成功，并且存放在了 这个文件下 /etc/letsencrypt/live/ssl.huiyanxian.cn/fullchain.pem

3、 合成tomcat的证书，在 tomcat 底下创建一个文件夹用来存放准备生产的证书（当然也可以自己择一个目录存放）

我的目录是：/usr/local/tomcat/conf/LetsEncrypt ，

```
#进入申请证书的目录，这个目录会以第一个域名明明，不影响多域名使用。
cd /etc/letsencrypt/live/ssl.huiyanxian.cn/

#复制到tomcat刚创建的证书目录下
cp fullchain.pem  /usr/local/tomcat/conf/LetsEncrypt

cp privkey.pem  /usr/local/tomcat/conf/LetsEncrypt

#进入到这个目录
cd /usr/local/tomcat/conf/LetsEncrypt/

#生成.p12文件
openssl pkcs12 -export -in fullchain.pem -inkey privkey.pem -out fullchain_and_key.p12 -n
```

me tomcat

这里会被要求设置密码，输入就行（下面用到的：yourPKCS12pass）

```
#生成.jks证书
keytool -importkeystore -deststorepass 'yourJKSpass' -destkeypass 'yourKeyPass' -destkeystore MyDSKeyStore.jks -srckeystore fullchain_and_key.p12

srcstoretype PKCS12 -srcstorepass 'yourPKCS12pass' -alias tomcat
```

其中 yourPKCS12pass 是上一步中设置的ssl证书密码，这里的yourKeyPass是要设置的keystore码，可以与yourPKCS12pass一致，下面配置tomcat会用到

4、 配置tomcat

```
<Connector port="80" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="443" />

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150" scheme="https" secure="true"
    keystoreFile="/usr/local/tomcat/conf/LetsEncrypt/MyDSKeyStore.jks" keystorePass="证的密码"
    clientAuth="false" sslProtocol="TLS" />
```

5、 完成，在tomcat创建两个站点，放入一个简单的.jsp文件，可以通过https://ssl.huiyanxian.cn https://tssl.huiyanxian.cn 即可访问。

免费证书只能用三个月，但是可以通过脚本自动更新，后续我会补充相关的自动更新的方法。

参考文献

1、certbot官方

2、更新python

3、配置生成证书