



链滴

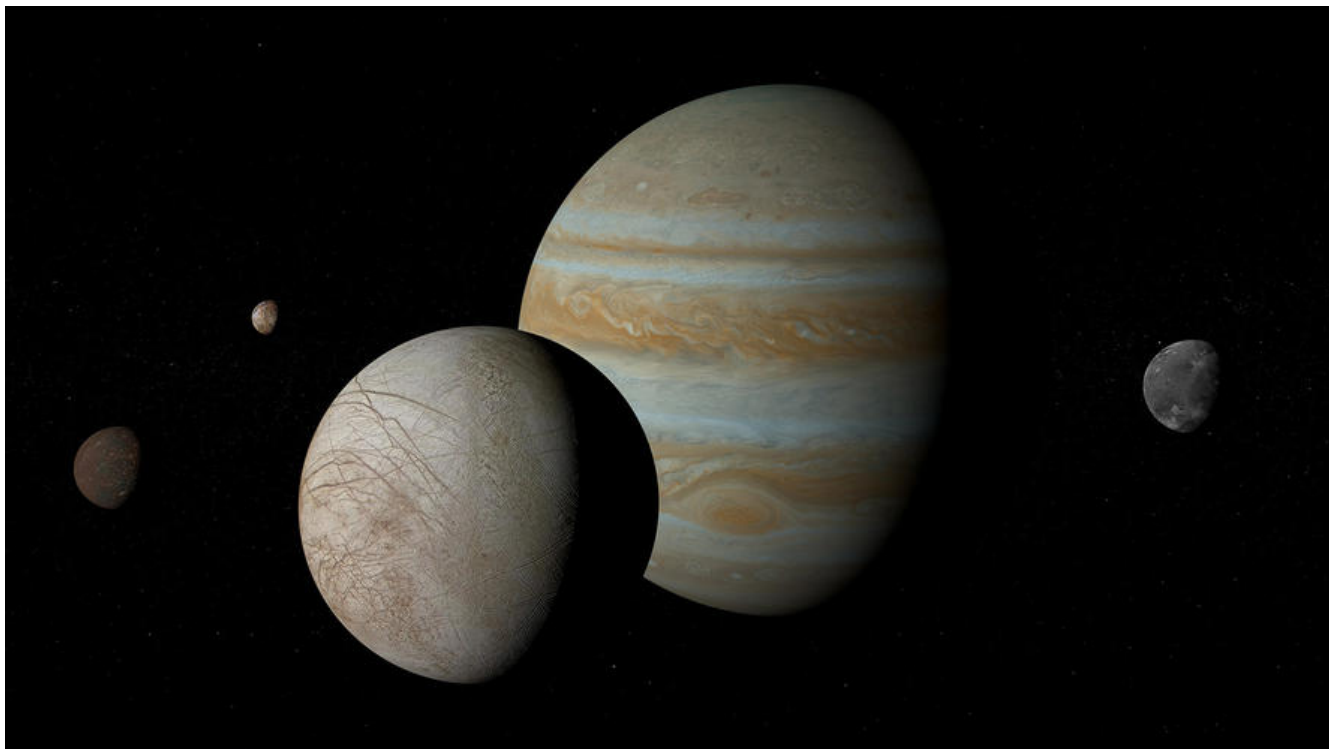
HTTP 申请 SSL 证书向 HTTPS 升级

作者: [smileLeol](#)

原文链接: <https://ld246.com/article/1590825236457>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)



前段时间，阿里云提醒SSL证书快过期了，当时项目在忙，没时间处理。趁着周末，申请下SSL证书处下该问题，特此记录下流程。

1.申请证书

SSL证书是数字证书的一种，因为配置在服务器上，也称为SSL服务器证书。因为阿里云上可以直接申请证书，故直接在其上搜索申请。

申请步骤如下：

1.购买证书

选择相关产品，按需购买，本人选择是免费的一款。

云盾证书服务(包年)

产品详情

产品文档

产品控制台

选择域名类型

通配符域名 (推荐)

单域名

多域名

保护一个单页面网站。例如 domain.com, ssl.domain.com, ssl.ssl.domain.com。如需保护网站下的所有子域名，请购买通配符证书。
仅GlobalSign OV证书支持OV证书。其他品牌的单域名证书暂时不支持OV证书。

选择证书类型

OV SSL

OV SSL

EV SSL

通过验证您的域名，为您提供证书，保护您的数据安全，同时可提高您网站的信誉排名。
OV SSL是企业/个人为验证其网站身份提供公信力的基础保证。拥有它才意味着您的网站所有权已经过严格审查。
如果您的域名含有.edu, .gov, .org, .jp (国家缩写), .pay, .bank, .live, .nuclear等特殊词，签发机构需要人工严格验证您的身份，为避免签发失败，请直接购买OV SSL证书。

选择加密等级

基础版

免费版

仅供个人或企业测试使用，扩展性较差且具有一定的安全隐患。
不支持IP证书。IP证书支持仅GlobalSign OV单域名证书。
每个UID仅支持签发20张OV单域名证书，可以购买OV基础版获得更多的OV单域名证书。

选择证书品牌

DigiCert

DigiCert是业界最受信任且广受赞誉的高保真证书提供商。
为89%的财富500强企业、全球前100大银行中的97家银行以及全球87%的加密电子商务交易提供保护。

选择域名个数

1

个

购买数量

1

+

购买时长

1年

证书签发日起1年有效期 (支持5天无理由退款)

总配置费用

¥0.00

立即购买

加入购物车

2.证书申请

点击证书申请，填入相关信息，等待审批就可以使用啦

未签发				
证书	绑定域名	已部署	状态	操作
DigiCert 免费版 SSL 实例: cas-cn-6jatobh5q0iy 有效期至: 1 年 标签: 未设置标签		--	已付款	证书申请 详情 升级

3.下载证书

下载证书放到服务器，开始进行下一步操作。

证书	绑定域名	已部署	到期时间	状态	操作
DigiCert 免费版 SSL 实例: cas-cn-6jatobh5q0iy 有效期至: 1 年 标签: 未设置标签	www.lhstudy.com lhstudy.com	--	2021年5月30日	已签发	详情 部署 下载 吊销

2.服务器配置

SSL证书可以在tomcat, nginx, apache等等都可以进行配置。我这里使用的是nginx。故记录的是nginx的配置过程。

一顿操作下，配置好后，发现nginx启动报错，原来，需要nginx开启ssl模块。onfused

```
[root@localhost ~]# ./sbin/nginx -s reload
nginx: [emerg] the "ssl" parameter requires ngx_http_ssl_module in /usr/local/nginx/conf/nginx.conf:114
```

操作步骤:

进入之前的nginx目录

```
cd /home/nginx-1.16.0
```

配置configure

```
./configure --prefix=/usr/local/nginx --with-http_stub_status_module --with-http_ssl_module
```

make

make

不能执行make install 会覆盖安装 ~

停止nginx，并替换之前的nginx

```
/usr/local/nginx/sbin/nginx -s stop
```

```
mv /usr/local/nginx/sbin/nginx /usr/local/nginx/sbin/nginx_bak
```

```
cp /home/nginx-1.16.0/objs/nginx /usr/local/nginx/sbin/nginx
```

查看安装情况

```
/usr/local/nginx/sbin/nginx -V
```

nginx version: nginx/1.16.0

built by gcc 4.4.7 20120313 (Red Hat 4.4.7-23) (GCC)

built with OpenSSL 1.0.1e-fips 11 Feb 2013

TLS SNI support enabled

configure arguments: --prefix=/usr/local/nginx --with-http_stub_status_module --with-http_ssl

_module

3.配置nginx

配置/usr/local/nginx/conf/nginx.conf文件

配置信息如下：

```
upstream tomcatServer{
    server localhost:8080;
}

server {
    #http跳转到https
    listen 80 ;
    server_name www.lhlstudy.com;
    rewrite ^/(.*)$ https://www.lhlstudy.com:443$1 permanent;
}
server {
    #可以配置为http与https 同时存在的情况，这里配置为http强制跳转至https
    #listen 80;
    listen 443 ssl;
    server_name www.lhlstudy.com ;

    ssl_certificate    cert/study.pem;
    ssl_certificate_key cert/study.key;

    ssl_session_timeout 5m;
    #使用此加密套件。
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!M
5:!ADH:!RC4;
    #使用该协议进行配置。
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_prefer_server_ciphers on;

    location / {

        proxy_redirect off;
        #可以配置至页面静态地址，由于这里是tomcat启动，配置tomcat访问代理
        proxy_pass http://tomcatServer;
        # proxy_set_header Host $host;
        proxy_set_header Host $host:$server_port;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }

    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
        root html;
    }
}
```

检测配置文件是否正确

```
/usr/local/nginx/sbin/nginx -t
```

重启nginx

```
/usr/local/nginx/sbin/nginx -s reload
```

4.打开页面检测

打开主页发现页面格式错乱，通过控制台发现页面资源文件还是指向http，才想起solo的博客需要在lake.properties配置文件中修改serverScheme=https。设置后，重启服务。解决问题！